使用Firepower威胁防御捕获和Packet Tracer

目录 <u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>FTD数据包处理</u> 配置 网络图 <u>使用Snort引擎捕获</u> 先决条件 <u>要求</u> <u>解决方案</u> <u>使用Snort引擎捕获</u> <u>要求</u> <u>解决方案</u> <u>Tcpdump过滤器示例</u> 使用FTD LINA引擎捕获 要求 <u>解决方案</u> 使用FTD LINA引擎捕获 — 通过HTTP导出捕获 要求 <u>解决方案</u> 使用FTD LINA引擎捕获 — 通过FTP/TFTP/SCP导出捕获 <u>要求</u> <u>解决方案</u> 使用FTD LINA引擎捕获 — 跟踪实际流量数据包 <u>要求</u> <u>解决方案</u> <u>6.2以后FMC软件版本中的捕获工具</u> <u>解决方法 — 使用FTD CLI</u> 在6.2之后FMC上跟踪实际数据包 FTD Packet Tracer实用程序 <u>要求</u> <u>解决方案</u> 6.2以后FMC软件版本的Packet Tracer UI工具 相关信息

简介

本文档介绍如何使用Firepower威胁防御(FTD)捕获和Packet Tracer实用程序。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本:

- 运行FTD软件6.1.0的ASA5515-X
- 运行FTD软件6.2.2的FPR4110
- 运行Firepower管理中心(FMC)软件6.2.2的FS4000

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

FTD数据包处理

FTD数据包处理可视化如下:



- 1. 数据包进入入口接口,由LINA引擎处理。
- 2. 如果策略要求数据包由Snort引擎进行检查。
- 3. Snort引擎返回数据包的判定。
- 4. LINA 引擎根据 Snort 的判定丢弃或转发数据包.

基于该体系结构,可以在以下位置获取FTD捕获:



配置

网络图



使用Snort引擎捕获

先决条件

在FTD上应用访问控制策略(ACP),允许互联网控制消息协议(ICMP)流量通过。该策略还应用了入 侵策略:

Overview	v Analysis	Pol	icies	Devices	Objects	AMP						(Deploy	/ 0	System	Help 🛛	mikis v
Access C	ontrol + Acco	ss Co	ntrol	Network	Discovery	Application Det	ectors	Co	rrelatio	n /	ctions •						
FTD55	15															Save	😫 Cancel
Enter a des	ription																
Identity Po	Identity Policy: None SSL Policy: None																
												Te	Inherita	nce Setti	ngs 📑 P	olicy Assi	gnments (1)
Rules	Security Inte	ligence	: HT	TP Response	s Advan	ced											
🛗 Filter b	y Device								O A	dd Cate	gory 🔾	Add Ruk	e Sea	rch Rules			×
# Name	1	s z	D Z	Source Networks	De	st tworks	v	u	A	Sr	Dest P	u	IS	Action			
👻 Manda	tory - FTD55	5-(1-)	ı)									_			_		
1 Allow	CMP	any	any	2 192.168.	103.0/24 👳	192.168.101.0/24	any	any	any	any	👷 ICMP (1) any	any	🗸 Aliov	V	1	J 🖯
👻 Defau	t - FTD5515 ()															
There are	no rules in this	section	n. Add R	ule or Add Ca	tegory								l l	ntrus	sion	Poli	cy 📃
Default A	tion								A	ccess (Control: Bloc	k All Traf	ffic				× 🗾

要求

- 1. 在FTD CLISH模式下启用捕获,无需过滤器。
- 2. 通过FTD ping并检查捕获的输出。

解决方案

步骤1:登录到FTD控制台或SSH到br1接口,并在FTD CLISH模式下启用捕获功能,无需过滤器。

<#root>

>

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection?
1
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

在FTD 6.0.x上,命令为:

<#root>

>

system support

capture-traffic

第二步:通过FTD Ping并检查捕获的输出。

<#root>

>

capture-traffic

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
```

Selection?

1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

```
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 1, let
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 1, let
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 2, let
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 3, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 3, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, let
12:52:34.759955 IP olab-vl647-gw.cisco.com
```

使用Snort引擎捕获

要求

1. 在FTD CLISH模式下使用IP 192.168.101.1过滤器启用捕获。

2. 通过FTD Ping并检查捕获的输出。

解决方案

步骤1:在FTD CLISH模式下使用IP 192.168.101.1过滤器启用捕获。

<#root>

>

capture-traffic

```
Please choose domain to capture traffic from:
```

0 - br1 1 - Router

Selection?

1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

host 192.168.101.1

第二步:通过FTD Ping并检查捕获的输出:

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 0, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 1, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 2, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len
```

可以使用-n选项查看数字格式的主机和端口号。例如,早期的捕获显示为:

<#root>

>

capture-traffic

Please choose domain to capture traffic from: 0 - br1 1 - Router Selection? 1 Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options: -n host 192.168.101.1 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80

Tcpdump过滤器示例

示例1:

要捕获Src IP或Dst IP = 192.168.101.1和Src port或Dst port = TCP/UDP 23,请输入以下命令:

<#root>

Options:

-n host 192.168.101.1 and port 23

示例 2:

要捕获Src IP = 192.168.101.1和Src port = TCP/UDP 23, 请输入以下命令:

<#root>

Options:

-n src 192.168.101.1 and src port 23

示例3:

要捕获Src IP = 192.168.101.1和Src port = TCP 23,请输入以下命令:

<#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

示例 4:

要捕获Src IP = 192.168.101.1并查看数据包的MAC地址,请添加"e"选项,然后输入以下命令:

<#root>

Options:

-ne

src 192.168.101.1

17:57:48.709954

6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90,

ethertype IPv4 (0x0800), length 58: 192.168.101.1.23 > 192.168.103.1.25420: Flags [S.], seq 3694888749, ack 1562083610, win 8192, options [mss 1380], length 0

示例 5:

要在捕获10个数据包后退出,请输入以下命令:

<#root>

Options:

-n -c 10 src 192.168.101.1

18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768, length 18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 2 18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 10 18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0 18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 0 18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 2 18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0 18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 10 18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0 18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 10 18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 1 18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 1 18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0

示例 6:

要将捕获写入名称为capture.pcap的文件并通过FTP将其复制到远程服务器,请输入以下命令:

<#root>

Options:

-w capture.pcap host 192.168.101.1
CTRL + C <- to stop the capture
> file copy 10.229.22.136 ftp / capture.pcap

Enter password for ftp@10.229.22.136: Copying capture.pcap

Copy successful.

>

使用FTD LINA引擎捕获

要求

Ē

1.使用以下过滤器在FTD上启用两个捕获:

=

源 IP	192.168.103.1
目的 IP	192.168.101.1
协议	ICMP
接口	内部
源 IP	192.168.103.1
源 IP 目的 IP	192.168.103.1 192.168.101.1
源 IP 目的 IP 协议	192.168.103.1 192.168.101.1 ICMP

2.从Host-A(192.168.103.1)对Host-B(192.168.101.1)执行ping操作并检查捕获。

解决方案

步骤1:启用捕获:

<#root>

> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1

> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1

第二步:在CLI中检查捕获。

从Host-A ping Host-B:

C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data: Reply from 192.168.101.1: bytes=32 time=4ms TTL=255 Reply from 192.168.101.1: bytes=32 time=5ms TTL=255 Reply from 192.168.101.1: bytes=32 time=1ms TTL=255 Reply from 192.168.101.1: bytes=32 time=1ms TTL=255

<#root>

> show capture

capture CAPI type raw-data interface INSIDE [Capturing

- 752 bytes

]

match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing

- 720 bytes

]

match icmp host 192.168.101.1 host 192.168.103.1

由于INSIDE接口上的Dot1Q报头,两个捕获的大小不同,如下面的输出示例所示:

<#root>

> show capture CAPI

8 packets captured 1: 17:24:09.122338

```
802.1Q vlan#1577
```

```
P0 192.168.103.1 > 192.168.101.1: icmp: echo request
2: 17:24:09.123071 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
3: 17:24:10.121392 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
4: 17:24:10.122018 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
5: 17:24:11.119714 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
6: 17:24:11.120324 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
7: 17:24:12.133660 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo reply
8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request
8: packets shown
```

<#root>

> show capture CAPO

8 packets captured

1: 17:24:09.122765 192.168.103.1 > 192.168.101.1: icmp: echo request 2: 17:24:09.122994 192.168.101.1 > 192.168.103.1: icmp: echo reply 3: 17:24:10.121728 192.168.103.1 > 192.168.101.1: icmp: echo request 4: 17:24:10.121957 192.168.101.1 > 192.168.103.1: icmp: echo reply 5: 17:24:11.120034 192.168.103.1 > 192.168.101.1: icmp: echo request 6: 17:24:11.12063 192.168.101.1 > 192.168.103.1: icmp: echo reply 7: 17:24:12.133980 192.168.103.1 > 192.168.101.1: icmp: echo request 8: 17:24:12.134194 192.168.101.1 > 192.168.103.1: icmp: echo reply

8 packets shown

使用FTD LINA引擎捕获 — 通过HTTP导出捕获

要求

使用浏览器导出在前面的场景中获取的捕获。

解决方案

要使用浏览器导出捕获,您需要:

1. 启用HTTPS服务器

2. 允许HTTPS访问

默认情况下,HTTPS服务器处于禁用状态,且不允许访问:

<#root>

>

show running-config http

>

步骤1:导航到设备>平台设置,单击新策略,然后选择威胁防御设置:

D	evices	Objects	AMP	Deploy) 📀	System	Help 🔻	mikis 🔻
PN	Platfor	m Settings						
							Object Ma	nagement
							📀 New I	Policy
	Device	Туре		Status		Firepower Settings		s
	Threat D	efense		Targeting 1 d	levice	Threat	Defense S	ettings

指定策略名称和设备目标:

New Policy		
Name:	FTD5515-System_Policy	
Description:		
Targeted Devices		
Select devices to	which you want to apply this policy.	
Available Devices	Selected Devices	
Search by nam	e or value	FTD5515

第二步:启用HTTPS服务器并添加要允许通过HTTPS访问FTD设备的网络:

Overview Analysis Policie	S Devices Objects AMP		
FTD5515-System_Po	licy		
ARP Inspection Banner External Authentication Fragment Settings HITP 1	Enable HTTP Server 7 2 Port 443 (P)	lease don't use 80 or 143)	3 🙆 Add
ICMP	Interface	Network	
Secure Shell SMTP Server	INSIDE	Net_192.168.103.0_24bits	/ 8

保存并部署。

在策略部署时,可以启用debug http以查看HTTP服务的启动:

> debug http 255

debug http enabled at level 255.

http_enable: Enabling HTTP server HTTP server starting.

FTD CLI的结果是:

<#root>

> unebug all

> show run http http server enable http 192.168.103.0 255.255.255.0 INSIDE

在Host-A(192.168.103.1)上打开浏览器,使用此URL下载第一个捕获 :<u>https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap</u>。

thtps://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	
Opening CAPI.pcap	
You have chosen to open:	
CAPLpcap	
which is: Wireshark capture file (776 bytes)	
What should Fireford a with this file?	
what should Firefox do with this file:	
Open with Wireshark (default)	
Save File	
Do this <u>a</u> utomatically for files like this from now on.	
OK Cancel	

供参考:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pca	2 启用HTTP服务器的FTD数据接口的
---	-------------------------

_



对于第二次捕获,请使用<u>https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap</u>。

O https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap
Opening CAPO.pcap
You have chosen to open:
CAPO.pcap
which is: Wireshark capture file (744 bytes) from: https://192.168.103.62
What should Firefox do with this file?
Open with Wireshark (default)
Save File
Do this automatically for files like this from now on.
OK Cancel

使用FTD LINA引擎捕获 — 通过FTP/TFTP/SCP导出捕获

要求

使用FTP/TFTP/SCP协议导出在早期场景中获取的捕获。

解决方案

将捕获导出到FTP服务器:

<#root>

firepower

copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination username [ftp_username]?

Destination password [ftp_password]?

Destination filename [CAPI.pcap]?
!!!!!!

114 packets copied in 0.170 secs

firepower#

将捕获导出到TFTP服务器:

<#root>

firepower

copy /pcap capture:CAPI tftp://192.168.78.73

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination filename [CAPI]?

346 packets copied in 0.90 secs

firepower#

将捕获导出到SCP服务器:

<#root>

```
firepower#
```

copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55

Source capture name [CAPI]?

Address or name of remote host [192.168.78.55]?

Destination username [scp_username]?

Destination filename [CAPI]? The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established. RSA key fingerprint is <cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:4 Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.

454 packets copied in 3.950 secs (151 packets/sec)

firepower#

从FTD卸载捕获。 目前,当您需要从FTD卸载捕获时,最简单的方法是执行以下步骤:

1.从Lina - copy /pcap capture:<cap_name> disk0:

2.从FPR根 — mv /ngfw/mnt/disk0/<cap_name> /ngfw/var/common/

3.从FMC UI - System > Health > Monitor > Device > Advanced Troubleshooting,然后在字段中输 入<cap_name>并下载。

使用FTD LINA引擎捕获 — 跟踪实际流量数据包

要求

使用以下过滤器在FTD上启用捕获:

源 IP	192.168.103.1
目的 IP	192.168.101.1
协议	ICMP
接口	内部
数据包跟踪	是
跟踪数据包的数量	100

从Host-A(192.168.103.1)Host-B(192.168.101.1)执行ping操作并检查捕获。

解决方案

跟踪实际数据包对于排除连接问题非常有用。它允许您查看数据包经过的所有内部检查。添加trace detail关键字并指定要跟踪的数据包数量。默认情况下,FTD跟踪前50个入口数据包。

在这种情况下,为FTD在INSIDE接口上接收的前100个数据包启用带有跟踪详细信息的捕获:

<#root>

> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168

从Host-A ping Host-B并检查结果:

C∶∖Use	rs/c :	isco>ping	192.10	58.101.1		
Pingin	g 192	2.168.101	.1 wit]	h 32 bytes	of data	
Reply	from	192.168.1	101.1:	bytes=32	time=2ms	TTL=255
Reply	from	192.168.1	101.1:	bytes=32	time=2ms	TTL=255
Reply	from	192.168.1	101.1:	bytes=32	time=2ms	TTL=255
Reply	from	192.168.1	101.1:	bytes=32	time=8ms	TTL=255

捕获的数据包包括:

<#root>

> show capture CAPI2

8 packets captured

1:	18:08:04.232989	802.1Q v1an#1577	P0	192.168.103.1 >	>	192.168.101.1:	icmp:	echo	request
2:	18:08:04.234622	802.1Q vlan#1577	P0	192.168.101.1 >	>	192.168.103.1:	icmp:	echo	reply
3:	18:08:05.223941	802.1Q vlan#1577	P0	192.168.103.1 >	>	192.168.101.1:	icmp:	echo	request
4:	18:08:05.224872	802.1Q vlan#1577	P0	192.168.101.1 >	>	192.168.103.1:	icmp:	echo	reply
5:	18:08:06.222309	802.1Q vlan#1577	P0	192.168.103.1 >	>	192.168.101.1:	icmp:	echo	request
6:	18:08:06.223148	802.1Q vlan#1577	P0	192.168.101.1 >	>	192.168.103.1:	icmp:	echo	reply
7:	18:08:07.220752	802.1Q vlan#1577	P0	192.168.103.1 >	>	192.168.101.1:	icmp:	echo	request
8:	18:08:07.221561	802.1Q vlan#1577	P0	192.168.101.1 >	>	192.168.103.1:	icmp:	echo	reply
	ate chown								

8 packets shown

此输出显示第一个数据包的跟踪。感兴趣的部分:

- 在第12阶段,可以看到"正向流"。这是LINA引擎调度阵列(实际上是指内部操作顺序)。
- 阶段13是FTD将数据包发送到Snort实例的位置。
- 在第14阶段,可以看到Snort判定。

<#root>

> show capture CAPI2 packet-number 1 trace detail

8 packets captured 1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346) Phase: 1 Type: CAPTURE ... output omitted ... Phase: 12 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 195, packet dispatched to next module Module information for forward flow ... snp_fp_inspect_ip_options snp_fp_snort snp_fp_inspect_icmp snp_fp_adjacency snp_fp_fragment snp_ifc_stat Module information for reverse flow ... snp_fp_inspect_ip_options snp_fp_inspect_icmp snp_fp_snort snp_fp_adjacency snp fp fragment snp_ifc_stat Phase: 13 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect' Phase: 14 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Verdict: (pass-packet) allow this packet ... output omitted ... Result: input-interface: OUTSIDE input-status: up input-line-status: up output-interface: OUTSIDE output-status: up output-line-status: up Action: allow 1 packet shown

6.2以后FMC软件版本中的捕获工具

在FMC版本6.2.x中,引入了一个新的数据包捕获向导。导航到设备>设备管理,然后单击故障排除 图标。然后选择Advanced Troubleshooting,最后选择Capture w/Trace。

Overview Analysis	Policies Devices	Objects	s AM	P Inte	lligence				
Device Management	NAT VPN VQ	os pi	atform S	ettings	FlexConf	ig (Certificates		
By Group 🗸									
Name		Group	Model	License	Туре	Acces	s Control Poli.		
FTD4110-2 10.48.23.254 - C	isco Firepower 4110 Threat	Cisco	Firepower	411(Bas	e, Threat, Ma	э	ACP1	P	6 🔀

选择Add Capture以创建FTD捕获:

Advanced Troubleshooting FTD4110-2												
Fil	e Download	Threat Defen	ise CLI	Packet	Tracer	Capture	w/Trace					
¢	C Auto Refresh Interval (seconds): 10 Enable Auto Refresh										ıre	
Na	Interface	Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status	

Add Capture				? : ×	
Name*:	САРІ	Interface*:	INSIDE		Source interface
Match Criteria:					
Protocol*:	IP 💌	•			IP Protocol
Source Host*:	192.168.0.10	Source Network:	255.255.255.255		
Destination Host*:	192.168.2.10	Destination Network:	255.255.255.255		
SGT number:	0	(0-65535)			Circular buffer
Buffer:					
Packet Size:	1518 14-1522 bytes	Continuous Ca	pture Trace		
Buffer Size:	524288 1534-33554432 bytes	Stop when full	Trace Cour	it: 50	

当前的FMC UI限制如下:

- 无法指定Src和Dst端口
- 只能匹配基本IP协议
- 无法为LINA引擎ASP丢弃启用捕获

解决方法 — 使用FTD CLI

从FMC UI应用捕获后,捕获会运行:

File D	ownload	Threat D	efense	CLI	Packet T	racer	Capture w,	/Trace		Clear the						
C Auto Refresh Interval (seconds): 10				Enable Au	to Refresh				capture				Add	Captu	ıre	
Na	Interface	Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status					
CAPI	INSIDE	raw-data	~	М	524288	1518	Capturing	IP	192.168.0.10	192.168.2.10	Running	Ø	6	->	11	
																Î
									[Pause the capture	Savo in po	e th cap	ie fo	cap rma	otui at	re

FTD CLI上的捕获:

<#root>

```
> show capture
```

```
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

在6.2之后FMC上跟踪实际数据包

在FMC 6.2.x上, Capture w/Trace向导允许您捕获和跟踪FTD上的实际数据包:

Add Capture			?	×
Name*:	CAPI	Interface*:	INSIDE	
Match Criteria:				
Protocol*:	IP 💌			
Source Host*:	192.168.16.111	Source Network:	255.255.255.255	
Destination Host*:	192.168.17.1	Destination Network:	255.255.255.255	
SGT number:	0	(0-65533)		
Buffer:				
Packet Size:	1518 14-1522 bytes	Continuous Car	oture 🕑 Trace	Trace ingress packets
Buffer Size:	524288 1534-33554432 bytes	Stop when full	Trace Count: 50	

您可以在FMC UI中检查跟踪的数据包:



FTD Packet Tracer实用程序

要求

使用Packet Tracer实用程序处理此流,并检查内部处理数据包的方式:

Ingress 接口	内部
协议	ICMP回应请求
源 IP	192.168.103.1
目的 IP	192.168.101.1

解决方案

Packet Tracer生成虚拟数据包。如本例所示,数据包接受Snort检测。在Snort级别同时捕获的捕获 (capture-traffic)显示ICMP回应请求: 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: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.101.1 using egress ifc OUTSIDE Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0 255.255.255.0 rule access-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1 access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMP Additional Information: This packet is sent to snort for additional processing where a verdict is reached ... output omitted ... Phase: 12 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 203, packet dispatched to next module Phase: 13 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: ICMP AppID: service ICMP (3501), application unknown (0) Firewall: allow rule, id 268440225, allow NAP id 2, IPS id 0, Verdict PASS

Snort Verdict: (pass-packet) allow this packet

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

>

Packet Tracer测试时的Snort级别捕获显示虚拟数据包:

<#root>

>

```
capture-traffic
```

```
Please choose domain to capture traffic from:
  0 - management0
  1 - Router
```

Selection? 1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
-n
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

6.2以后FMC软件版本的Packet Tracer UI工具

在FMC版本6.2.x中引入了Packet Tracer UI工具。该工具与捕获工具以相同的方式访问,并允许您 从FMC UI在FTD上运行Packet Tracer:

		Configurat	tion Users	Domains	Integration	Jpdates Lice	enses Health Monitor
Advanced Tro	oubleshooting						
File Download 1	Threat Defense CLI	acket Tracer	Capture v	v/Trace	Тр		e interface
Select the packet t	ype and supply the packet pa	rameters. Click	start to trace the	e packet.			
Packet type:	ТСР	~			Interface*:	INSIDE	~
Source*:	IP address (IPv4)	▼ 192.168	.0.10		Source Port*:	1111	~
Destination*:	IP address (IPv4)	▼ 192.168	.2.10		Destination Port*	t: http	~
SGT number:	SGT number. (0-65533)	VLAN ID	VLAN ID	(1-4096)	Destination Mac Address:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	00X
Output Format:	summary	~					
Start	Clear						
< Output				•			
output							Rav
Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Informatio MAC Access list	n:				The	tracer c	output

相关信息

- Firepower威胁防御命令参考指南
- <u>Firepower系统版本说明,版本6.1.0</u>
- 适用于Firepower设备管理器的思科Firepower威胁防御配置指南,版本6.1
- <u>技术支持和文档 Cisco Systems</u>

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)。