工作用FTD捕获和数据包追踪器

目录

简介

本文描述如何与Firepower威胁防御(FTD)捕获和数据包追踪器工具一起使用。

数据包捕获是其中一最常用的故障排除工具。使用案件数据包捕获是：

- 证明，数据包在设备到达
- 证明，数据包留下设备
- 要证明，数据包由设备丢弃(即ASA ASP丢弃)

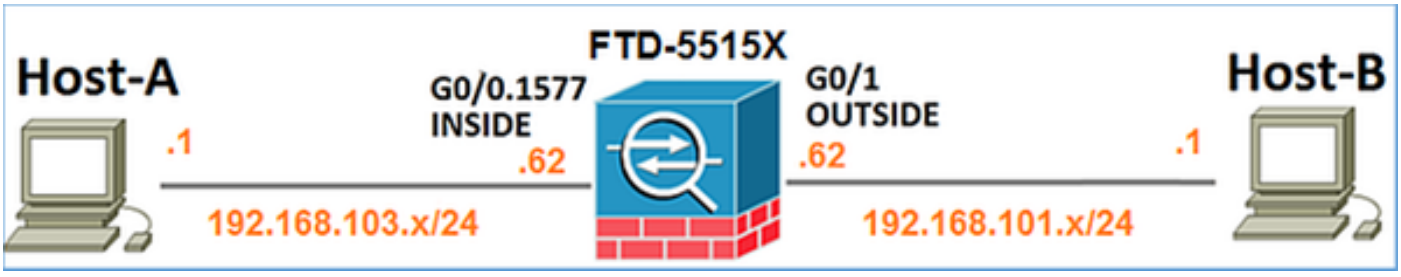
在FTD数据包可以乘两个引擎捕获：

1. ASA引擎
2. 喷鼻息引擎

使用的组件

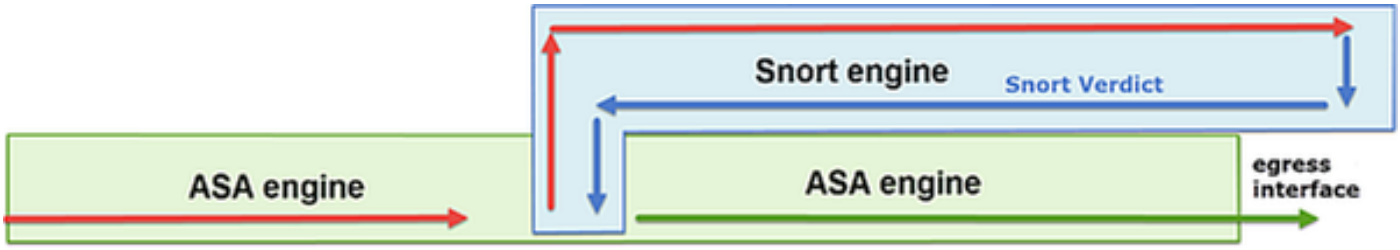
- 运行FTD代码6.1.0 (构建330)的ASA5515X
- 运行6.1.0的Firepower管理中心(FMC) (构建330)

拓扑



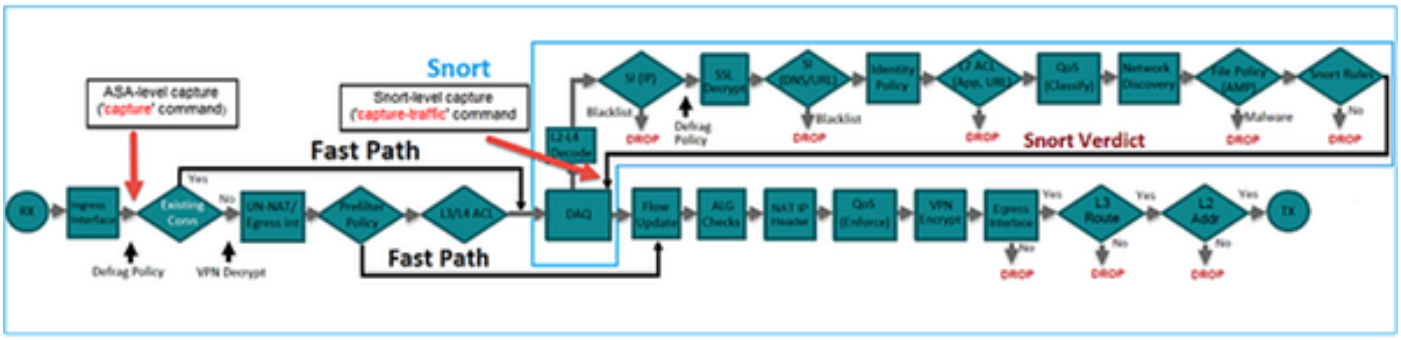
FTD数据包处理

FTD数据包处理可以形象化如下：



1. 数据包进入入口接口，并且乘ASA引擎处理
2. 如果策略指示数据包乘喷鼻息引擎检查
3. 喷鼻息引擎返回一个判决(即whitelist，黑名单)数据包的
4. ASA引擎丢弃或转发根据喷鼻息的判决的数据包

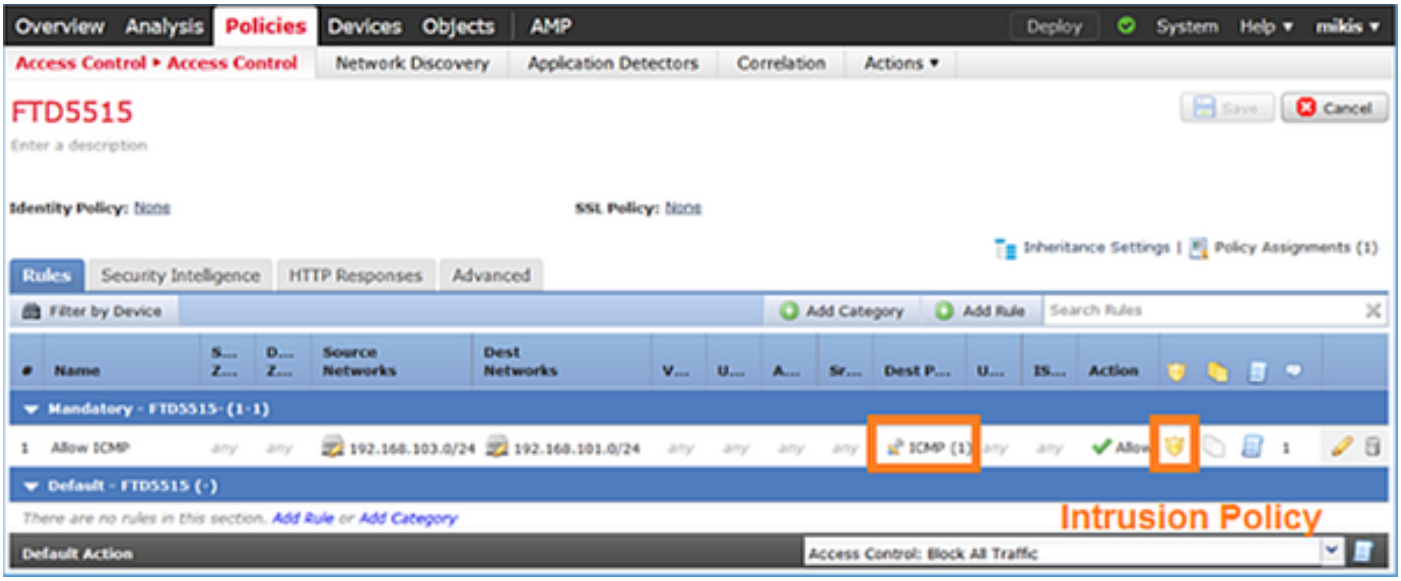
基于上述体系结构FTD捕获在2个不同的地方可以被采取：



工作与喷鼻息引擎捕获

[先决条件]

有在允许ICMP流量经历的FTD (非加太)应用的访问控制策略。策略也有应用的一项入侵策略：



要求

1. 在FTD CLISH模式的Enable (event)捕获使用没有过滤器
2. 通过FTD ping并且检查捕获输出

解决方案

步骤 1：FTD控制台的对br1接口和enable (event)捕获的洛金或SSH在FTD CLISH模式使用没有过滤器

```
> 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:
```

在FTD 6.0.x命令是：

```
> system support capture-traffic
```

步骤 2：通过FTD ping并且检查捕获输出

```
> 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, length 80 12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 0, seq 1, length 80 12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-
gw.cisco.com: ICMP echo request, id 0, seq 2, length 80 12:52:34.759955 IP olab-vl647-
gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, length 80 12:52:34.759955
IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, length 80
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
3, length 80 12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo
request, id 0, seq 4, length 80 12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 0, seq 4, length 80 ^C <- to exit press CTRL + C
```

工作与喷鼻息引擎捕获(用tcpdump过滤器)

要求

1. 启用在FTD CLISH模式的捕获使用IP的192.168.101.1一个过滤器
2. 通过FTD ping并且检查捕获输出

解决方案

步骤 1：启用在FTD CLISH模式的捕获使用IP的192.168.101.1一个过滤器

```
> 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
```

步骤 2：通过FTD ping并且检查输出的捕获：

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
0, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
1, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
2, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
3, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
4, length 80
```

您能使用“- n’选项发现主机和端口号在数字格式。例如上述捕获将显示如下：

```
> 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 4, length 80
```

Tcpdump过滤器示例

示例 1

捕获Src IP或Dst IP = 192.168.101.1和Src端口或者Dst port= TCP/UDP 23 ：

```
Options: -n host 192.168.101.1 and port 23
```

示例 2

捕获Src IP = 192.168.101.1和Src port= TCP/UDP 23 ：

```
Options: -n src 192.168.101.1 and src port 23
```

示例 3

捕获Src IP = 192.168.101.1和Src port= TCP 23 ：

```
Options: -n src 192.168.101.1 and tcp and src port 23
```

示例 4

捕获Src IP = 192.168.101.1和看到数据包的MAC地址添加'e'选项：

```
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

在捕获10数据包以后退出：

```
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 0 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 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 [P.], 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 [P.], ack 7, win 32768, length
12 18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768,
length 0
```

示例6

写捕获到有名称的capture.pcap一个文件和通过FTP复制它到远程服务器：

```
Options: -w capture.pcap host 192.168.101.1 CTRL + C <- to stop the capture > system file copy
10.229.22.136 ftp / capture.pcap Enter password for ftp@10.229.22.136: Copying capture.pcap Copy
successful. >
```

工作与FTD ASA引擎捕获

要求

1. Enable (event)在FTD的2个捕获使用以下过滤器：

源 IP	192.168.103.1
目的 IP	192.168.101.1
协议	ICMP
接口	里面
源 IP	192.168.103.1
目的 IP	192.168.101.1
协议	ICMP
接口	从外部

2. 从host-a (192.168.103.1) ping host-b (192.168.101.1)并且检查捕获。

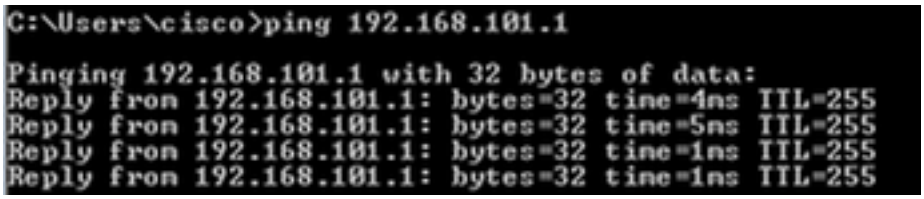
解决方案

步骤 1：启用捕获：

```
> 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
```

步骤 2：检查捕获使用CLI

从host-a的Ping到Host-B:




```
> 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
```

2个捕获有不同的大小由于在内部接口的Dot1q报头。这在以下输出中可以显示：

```
> 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 request 8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply 8 packets shown > 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: 17:24:11.120263 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
```

工作与FTD ASA引擎捕获–导出捕获使用HTTP

要求

导出在前一场景采取的捕获使用浏览器

解决方案

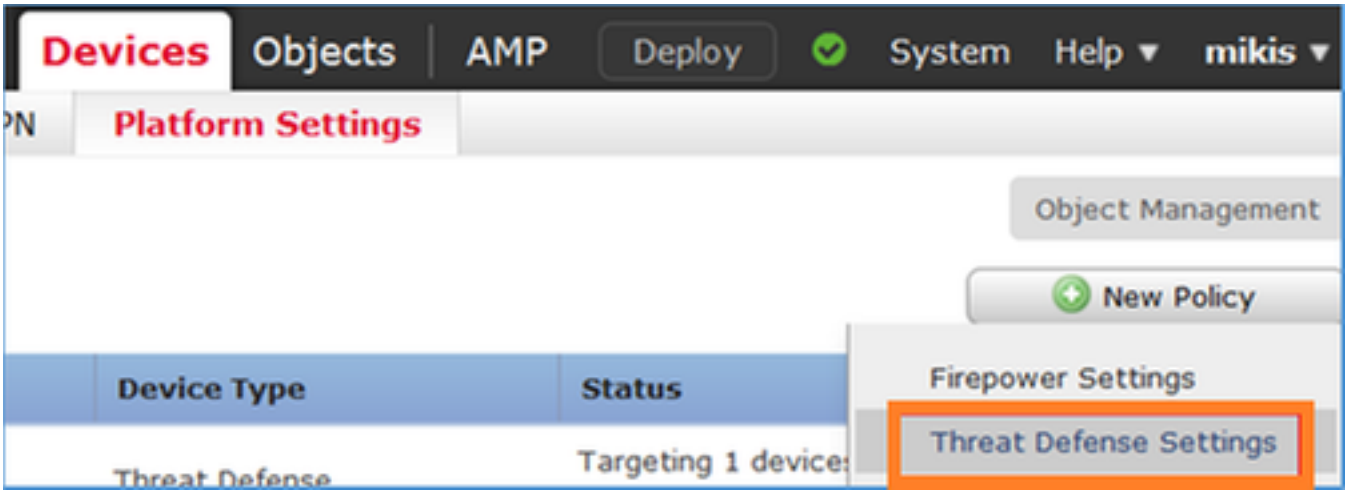
为了导出捕获使用那里浏览器是需要：

1. Enable (event) HTTPS服务器
2. 允许HTTPS访问

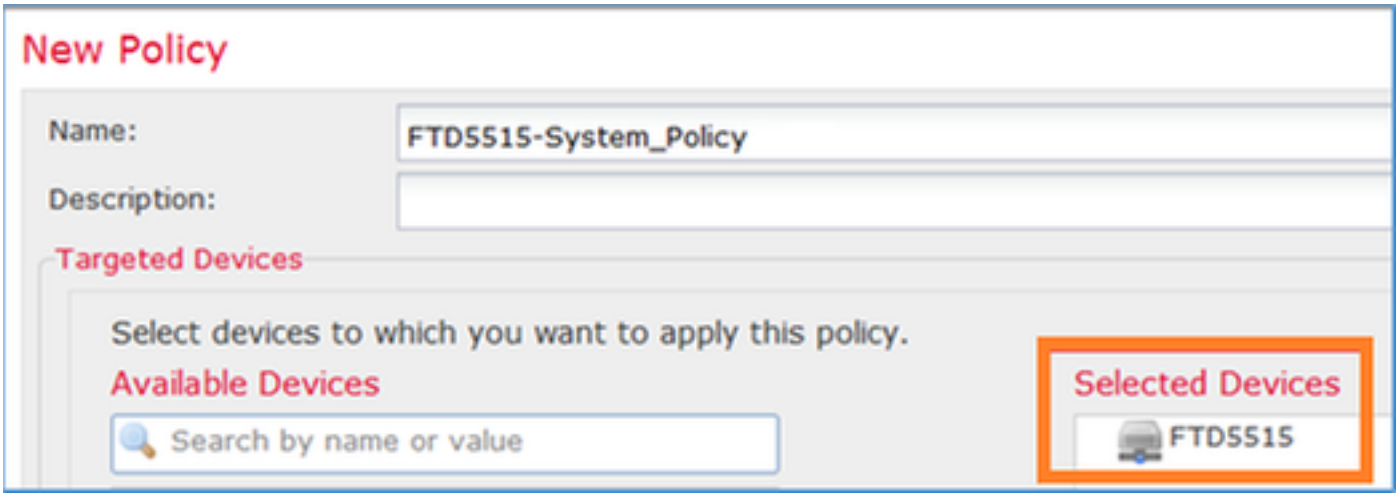
默认情况下HTTPS服务器禁用，并且访问没有允许：

```
> show running-config http
 >
```

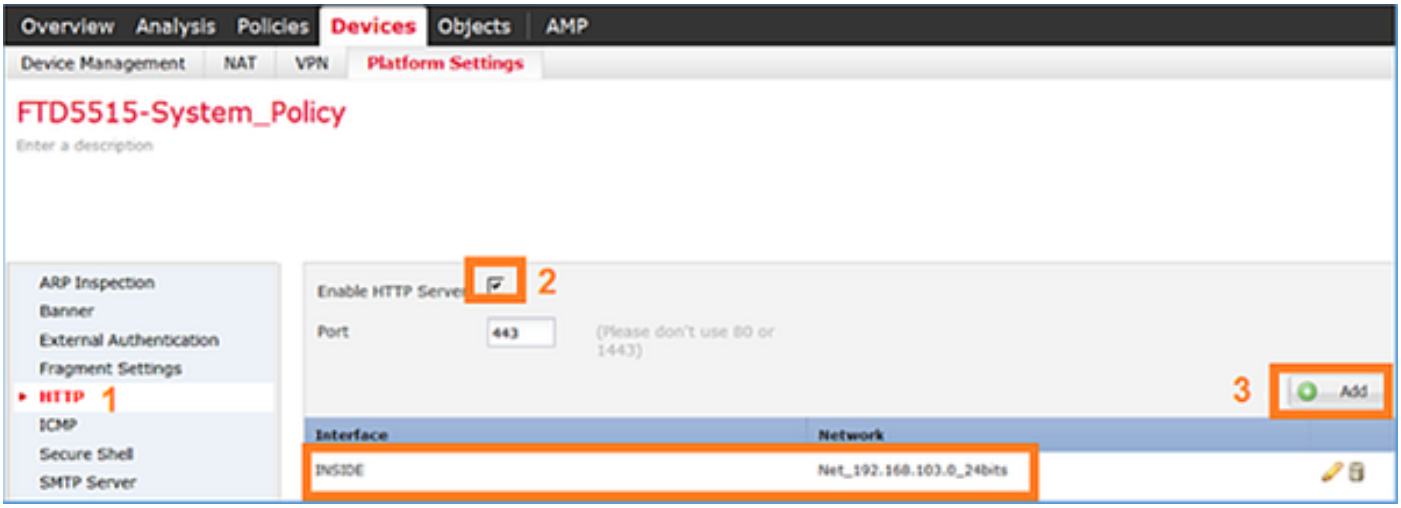
步骤 1：导航对**设备>平台设置，**点击**New策略**并且选择**威胁防御设置：**



指定策略名称和设备目标：



步骤 2：启用HTTPS服务器并且添加应该允许访问在HTTPS的FTD设备的网络：



保存并且**部署**

提示

当您部署策略时您能使**调试http**为了发现HTTP服务开始：

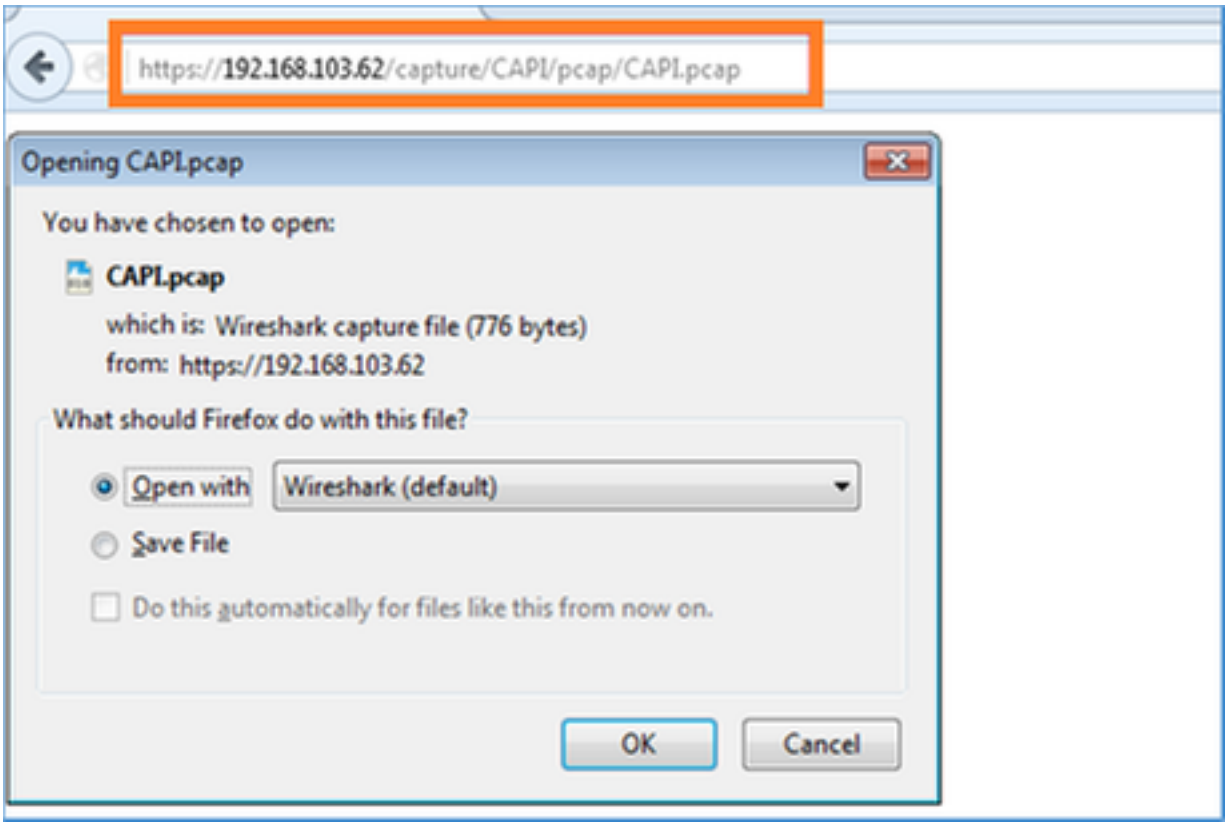
```
> debug http 255 debug http enabled at level 255. http_enable: Enabling HTTP server HTTP server starting.
```

这是在FTD CLI的结果：

```
> unebug all
> show run http http server enable http 192.168.103.0 255.255.255.0 INSIDE
```

打开在host-a的一个浏览器(192.168.103.1)并且请使用以下URL下载第一个捕获：

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap

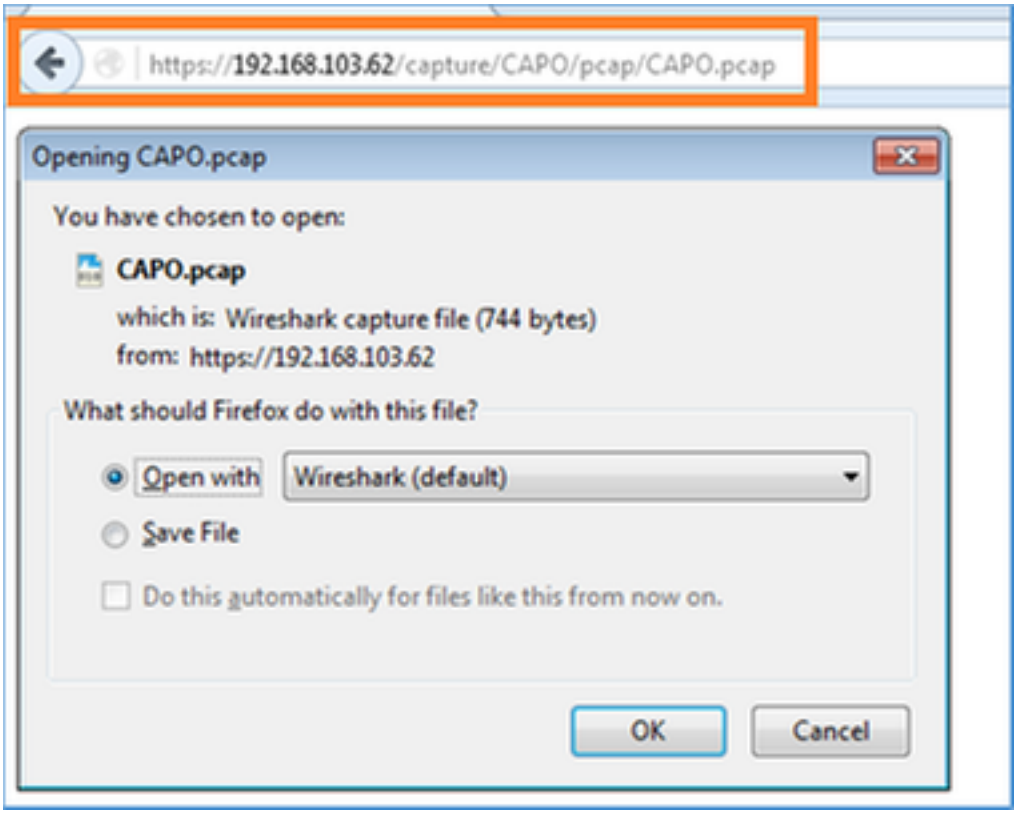


供参考

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	HTTP服务器启用FTD数据接口的IP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	FTD捕获的名称
https://192.168.103.62/capture/CAPI/pcap/ CAPI.pcap	将下载文件的名称

第二个捕获：

https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap



工作与FTD ASA引擎捕获–导出捕获使用FTP/TFTP/SCP

要求

导出在上一个方案采取的捕获使用FTP/TFTP/SCP协议

解决方案

导出对FTP服务器的一个捕获：

```
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#
```

导出对TFTP server的一个捕获：

```
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#
```

导出对SCP服务器的一个捕获：

```
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:49:9e:39:36:96:33
>(SHA256). 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#
```

工作与FTD ASA引擎捕获–跟踪数据包

要求

使用以下过滤器，启用在FTD的一个捕获：

源 IP	192.168.103.1
目的 IP	192.168.101.1
协议	ICMP
接口	里面
包跟踪	是
跟踪数据包编号	100

从host-a (192.168.103.1) ping host-b (192.168.101.1)并且检查捕获。

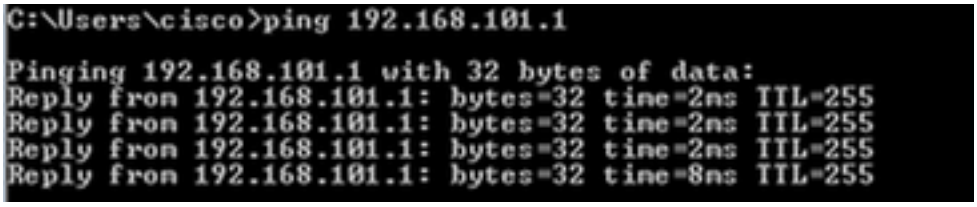
解决方案

跟踪实际数据包可以是非常有用的为排除故障连通性问题。它准许发现数据包通过的所有内部检查。添加“**trace详细信息**”关键字并且指定将跟踪的相当数量数据包。默认情况下FTD跟踪前50入口数据包。

在这种情况下与trace详细信息的enable (event)捕获FTD在内部接口收到的前100数据包的：

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168.101.1
```

从host-a ping到host-b并且检查结果：



这是获取数据包：

```
> show capture CAPI2 8 packets captured 1: 18:08:04.232989 802.1Q vlan#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 8 packets shown
```

这是第一数据包的trace。有趣的零件是：

- 相位12能被看到'向前流'的地方。这是ASA引擎分派阵列(有效内部运算顺序)
- 相位13 FTD发送数据包打鼾实例的地方
- 相位14喷鼻息判决被看到的地方

```
> 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 >
```

使用FTD数据包追踪器工具

要求

请使用数据包追踪器工具以下流并且检查数据包如何将被处理得内部地：

入口接口	里面
协议	ICMP echo请求
源 IP	192.168.103.1
目的 IP	192.168.101.1

解决方案

数据包追踪器将生成一**虚拟数据包。**当能在数据包之下被看到是打鼾的主题检查，但是在喷鼻息引擎的捕获显示虚拟数据包没有通过它实际上发送：

> **packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1** 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-id 268436482 event-log both 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 will be sent to snort for additional processing where a verdict will be 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 Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE output-status: up output-line-status: up Action: allow >

相关文档

Firepower威胁防御命令参考指南

Firepower系统版本笔记，版本6.1.0

Cisco Firepower威胁Firepower设备管理器的防御配置指南，版本6.1