# 在FMC中使用Packet Tracer工具重播数据包

### 目录

 箇介

 先决条件

 要求

 使用的组件

 使用FMC上提供的Packet Tracer工具重播数据包

 使用PCAP文件重播数据包

 使用此选项的限制

 相关文档

### 简介

本文档介绍如何使用FMC GUI Packet Tracer工具在FTD设备中重播数据包。

## 先决条件

#### 要求

Cisco 建议您了解以下主题:

- Firepower技术知识
- 了解通过防火墙的数据包

#### 使用的组件

- 思科安全防火墙管理中心(FMC)和思科防火墙威胁防御(FTD) 7.1版或更高版本。
- PCAP格式的数据包捕获文件

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。

### 使用FMC上提供的Packet Tracer工具重播数据包

1. 登录FMC GUI。转至Devices > Troubleshoot > Packet Tracer。

|               | Firewall Management Center Overview Analysis Policies Devices / Troubleshoot / Packet Tracer   | Devices Objects Inter  | gration  | Deploy Q 🚱 🌣 🕼   | admin ~ shoth SECURE |
|---------------|--|--|--|--|----------------------|
| Trace History | New Trace       +         Select Device*       10.197.224.9         Select the packet type from the Protocol drop-down, and then specify the packet part         Protocol*       TCP         or       Select a PCAP File         Source Type*       IPv4         Source Port*       Enter or select a port number         Inline Tag       (0-65535)         Bypass security checks for the simulated packet | Device Management<br>NAT<br>QoS<br>Platform Settings<br>FlexConfig<br>Certificates | VPN<br>Site To Site<br>Remote Access<br>Dynamic Access Policy<br>Troubleshooting | Troubleshoot<br>File Download<br>Threat Defense CLI<br>Packet Tracer<br>Packet Capture<br>Upgrade<br>Threat Defense Upgrade<br>Chassis Upgrade | CLI   Packet Capture |
|               | Treat the simulated packet as an IPsec/SSL VPN decrypted packet  |  |  |  | Reset                |
|               | Trace Result   |  |  |  | ¶a ⊗ ⊠               |
|               |  |  |  |  |                      |

#### 2. 提供源、目标、协议和入口接口的详细信息。点击Trace。

|         | Firewall Manager<br>Devices / Troubleshoot /  | ment Center<br>/ Packet Tracer | Overview   | Analysis    | Policies | Devices          | Objects    | Integration  | 1           | Deploy    | ۹ (   | p ¢       | admin     | eisco SECURE   |
|---------|---|--------------------------------|------------|-------------|----------|------------------|------------|--|-------------|-----------|-------|-----------|-----------|----------------|
| Ш       |   |                                |            |             |          |                  |            |  |             | File Dow  | nload | Threat De | fense CLI | Packet Capture |
| T.      | New Trace -   | +                              |            |             |          |                  |            |  |             |           |       |           |           |                |
| ice His | Select Device*  | 10.70.73.44                    |            | ×.          |          |                  | Ingress Ir | iterface*  | Select      |           |       | ∼ C       |           |                |
| tory    | Select the packet type from the Protocol drop-down, and then specify the packet parameters. |                                |            |             |          | VLAN ID (1-4096) |            |  |             |           |       |           |           |                |
|         | Protocol*   | ICMP ~                         | or Select  | a PCAP File | ~ 0      |                  |            |  |             |           |       |           |           |                |
|         | Source Type*  | IPv4 🗸                         | 192.168.1. | 2           |          |                  | Destinatio | on Type*   | IPv4 $\lor$ | 10.197    | 226.1 |           |           |                |
|         | Type*   | 8 (Echo Request)               |            | ~           |          |                  | ID         |  |             | ] (1-6553 | 5)    |           |           |                |
|         | Code*   | 0                              | (0-255)    |             |          |                  |            |  |             |           |       |           |           |                |
|         | Inline Tag  |                                | (0-65533)  |             |          |                  |            |  |             |           |       |           |           |                |
|         | Bypass security checks for the simulated packet   |                                |            |             |          |                  |            | Allow the simulated packet to transmit from the device |             |           |       |           |           |                |
|         | Treat the simulated packet as an IPsec/SSL VPN decrypted packet                             |                                |            |             |          |                  |            |  |             |           |       |           |           |                |
|         |   |                                |            |             |          |                  |            |  |             |           |       |           | Res       | et Trace       |
|         | Trace Result  |                                |            |             |          |                  |            |  |             |           |       |           |           | n. ∀ 55        |

3. 使用Allow the simulated packet to transmit from the device选项,从设备重播此数据包。 4. 请注意,数据包已丢弃,因为访问控制策略中配置了一条用于丢弃ICMP数据包的规则。

| Trace Result:         DROP           Tace Result:         DROP           Backet Details:         11:59:51.233 - 192.168.1.2 > 10.106.226.1 ICMP           PC(vrfid:0)         >           ACCESS-LIST         ACCESS-LIST   | Reset Trace |  |  |  |  |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|--|--|--|--|
| Trace Result         © DROP           Image: Packet Details: 11:59:51.233 - 192.168.1.2 > 10.106.226.1 ICMP           Image: PC(vrfid:0)           Image: PCCESS-LIST   | ¶∎ ⊗ ≫      |  |  |  |  |  |  |  |  |  |  |
| Image: Packet Details: 11:59:51.233 - 192.168.1.2 > 10.106.226.1 ICMP           Image: PC(vrfid:0)           > ⊘ ACCESS-LIST  |             |  |  |  |  |  |  |  |  |  |  |
| PC(vrfid:0)     ACCESS-LIST   |             |  |  |  |  |  |  |  |  |  |  |
| ACCESS-LIST   |             |  |  |  |  |  |  |  |  |  |  |
|   |             |  |  |  |  |  |  |  |  |  |  |
| > O INPUT-ROUTE-LOOKUP   Resolve Egress Interface   |             |  |  |  |  |  |  |  |  |  |  |
| ✓ ● ACCESS-LIST   log   |             |  |  |  |  |  |  |  |  |  |  |
| Type: ACCESS-LIST   |             |  |  |  |  |  |  |  |  |  |  |
| Subtype: log  |             |  |  |  |  |  |  |  |  |  |  |
| Result: ODP   |             |  |  |  |  |  |  |  |  |  |  |
| Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny object-group ICMP_ALLOW ifc PC any ifc OUT any rule-id 268454920 event-log flow-start<br>list CSM_FW_ACL_ remark rule-id 268454920; ACCESS POLICY: Port-scan test Mandatory access-list CSM_FW_ACL_ remark rule-id 268454920; L4 RULE: block ICMP |             |  |  |  |  |  |  |  |  |  |  |
| Additional Information  |             |  |  |  |  |  |  |  |  |  |  |
| Result: drop  |             |  |  |  |  |  |  |  |  |  |  |
| Input Interface: PC(vrfid:0)  |             |  |  |  |  |  |  |  |  |  |  |
| Input Status: up  |             |  |  |  |  |  |  |  |  |  |  |
| Input Line Status: up   |             |  |  |  |  |  |  |  |  |  |  |
| Output Interface: OUT(vrfid:0)  |             |  |  |  |  |  |  |  |  |  |  |
| Output Status: up   |             |  |  |  |  |  |  |  |  |  |  |
| Output Line Status: up  |             |  |  |  |  |  |  |  |  |  |  |
| Action: drop  |             |  |  |  |  |  |  |  |  |  |  |
| Drop Reason: (acl-drop) Flow is denied by configured rule   |             |  |  |  |  |  |  |  |  |  |  |
| Drop Detail: , Drop-location: frame 0x000000aaacdc0eb0 flow (NA)/NA   |             |  |  |  |  |  |  |  |  |  |  |
| OUT(vrfd:0)   |             |  |  |  |  |  |  |  |  |  |  |

#### 5. 此Packet Tracer使用TCP数据包跟踪的最终结果(如图所示)。

| þ           | Firewall Management Center         Overview         Analysis         Policies         Devices   | Objects Integration Deploy Q 🌮 🌣 🕢 admin V 🖓   |
|-------------|---|--|
| <br>        | New Trace +   | File Download   Threat Defense CLI   Packet Capture  |
| ace History | Select Device*     10.70.73.44       Select the packet type from the Protocol drop-down, and then specify the packet parameters.       Protocol*     TCP       Yor     Select a PCAP File   | Ingress Interface* PC - Ethernet1/1 VLAN ID (1-4096)   |
|             | Source Type*         IPv4         I92.168.1.2           Source Port*         1234         (0-65535)           Inline Tag         (0-65533)  | Destination Type*         IPv4         III.197.226.1           Destination Port*         443         (0-65535) |
|             | Bypass security checks for the simulated packet Treat the simulated packet as an IPsec/SSL VPN decrypted packet   | Allow the simulated packet to transmit from the device           Reset         Trace                           |
|             | Trace Result:         ALLOW           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:00.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:00.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:00.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:00.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP           Image: Packet Details:         12:03:00.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP <th>¶a ⊗ X</th> | ¶a ⊗ X   |
|             | > O ACCESS-LIST   log<br>> O CONN-SETTINGS  |  |

### 使用PCAP文件重播数据包

您可以使用Select a PCAP File(选择PCAP文件)按钮上传pcap文件。然后选择Ingress接口并点击Trace。

| p                                      | Firewall Manage<br>Devices / Troubleshoo                            | ement Center<br>t / Packet Tracer                       | Overview  | Analysis                                 | Policies Devices  | Objects Int                                | tegration         | Deploy Q                      | ¢ €         | admin 🗸         | eisco SECURE  |
|--|---|---|---|--|-------------------|--|-------------------|-------------------------------|-------------|-----------------|---------------|
| <br>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | New Trace 3   | +   |   |  |                   |  |                   | File Downloa                  | ad   Threat | Defense CLI   P | acket Capture |
| ace History                            | Select Device*<br>Select the packet ty<br>Protocol*<br>Source Type* | 10.197.224.9<br>ype from the Protocol dr<br>TCP<br>IPv4 | op-fown, and th                                       | en specify the particular to a PCAP File | acket parameters. | Ingress Interf<br>VLAN ID<br>Destination T | vpe* IPv4         | igabitEthernet0/1<br>(1-4096) | √ C         |                 |               |
|  | Source Port*<br>Inline Tag<br>Bypass security<br>Treat the simula   | checks for the simulate<br>ated packet as an IPsec/     | ort number<br>(0-65533)<br>d packet<br>SSL VPN decryp | v (0-6                                   | 5535)             | Destination P                              | ort* Enter or sel | ect a port number             | ~ (0        | -65535)         |               |
|  | Traco Bosult  |   |   |  |                   |  |                   |                               |             | Reset           | Trace         |
|  | nace result   |   |   |  |                   |  |                   |                               |             |                 |               |

### 使用此选项的限制

- 1. 我们只能模拟TCP/UDP数据包。
- 2. PCAP文件中支持的最大数据包数为100。

- 3. Pcap文件大小必须小于1 MB。
- 4. PCAP文件名不能超过64个字符(包括扩展名),并且只能包含字母数字、特殊字符("。"、"-"、"\_")或两者。
- 5. 当前仅支持单个流数据包。

#### 跟踪3将丢弃原因显示为无效IP报头

| þ      | Firewall Managen<br>Devices / Troubleshoot /    | nent Center<br>Packet Tracer   | Overview Anal  | sis Policies  | Devices 0                                 | Objects Inte                  | egration |  | Deploy Q   | 6 <sup>00</sup> ¢ | 🔞 admin 🗸 | cisco      | SECU  | ŧE |  |
|--------|---|--|--|---|---|-------------------------------|----------|--|------------|-------------------|-----------|------------|-------|----|--|
|        | Select the packet type                          | from the Protocol dro  | op-down, and then spe  | city the packet par   | ameters.                                  | VLAN ID                       |          |  | (1-4096)   |                   |           |            |       |    |  |
| ш      | Protocol*                                       | UDP  | v or single2.pcap  | ~   |   |                               |          |  |            |                   |           |            |       |    |  |
| Trac   | Source Type*                                    | IPv4   | v 192.168.29.58  |   |   | Destination Ty                | IP       | Pv4 ∨  | 192.168.29 | .160              |           |            |       |    |  |
| ен     | Source Port*                                    | 60376  |  | ✓ (0-65535)   |   | Destination Po                | ort* 16  | 61   | ✓ (0-65535 |                   |           | )          |       |    |  |
| istory | Inline Tag                                      |  | (0-65533)  |   |   |                               |          |  |            |                   |           |            |       |    |  |
|        | Bypass security checks for the simulated packet |  |  |   |   |                               |          | Allow the simulated packet to transmit from the device |            |                   |           |            |       |    |  |
|        | Treat the simulate                              | d packet as an IPsec/S   | SSL VPN decrypted pa   | :ket  |   |                               |          |  |            |                   |           |            |       |    |  |
|        |   |  |  |   |   |                               |          |  |            |                   | Reset     |            | Trace |    |  |
|        | Trace Result: 49 Erro                           | r: Some packets from   | the PCAP file were no  | replayed.   |   |                               |          |  |            |                   |           | F <u>B</u> | × ×   |    |  |
| - 1    | Packet 1: 11:58:21.8                            | 75534 🔥 Packe  | et Details: 11:58:21.87  | 5534 192.168.29.5   | 58:60376 > 192.168                        | 3.29.160:161 ud               | p 80     |  |            |                   |           |            |       |    |  |
|        |   | <ul> <li>inside</li> <li>Result</li> <li>Result</li> <li>Inp</li> <li>Inp</li> <li>Inp</li> <li>Out</li> <li>Act</li> <li>Tim</li> <li>Drc</li> <li>NP Id</li> </ul> | e(vrfid:0)<br>t: drop<br>put Interface:<br>put Status:<br>put Line Status:<br>tput Interface;<br>tion:<br>ne Taken:<br>op Reason:<br>op Detail:<br>lentity Ifc | inside(vrfid:0)<br>up<br>NP Identity Ifc<br>drop<br>O ns<br>(invalid-ip-hea<br>Drop-location: | nder) Invalid IP hea<br>frame 0x000055f7c | <b>der</b><br>fb1b71b flow (N | ła)/NA   |  |            |                   |           |            |       |    |  |

# 相关文档

有关数据包捕获和跟踪器的详细信息,请参阅<u>Cisco Live文档</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)。