使用Umbrella排除FTD注册问题

目录

问题

Umbrella网络设备控制面板显示已集成和连接的思科防火墙管理中心(FMC)。FMC还可以将Umbrella策略拉到FMC并将其部署到思科防火墙威胁防御(FTD)。但是，FTD无法注册到Umbrella以重定向DNS流量。

环境

- 思科安全防火墙Firepower FTD 10.0.0（适用于版本7.2+）
- 防火墙管理中心(FMC)版本10.0.0（适用于版本7.2+）
- 在Azure虚拟WAN环境中部署（也适用于硬件型号）
- FMC已成功与思科Umbrella集成
- FTD上的Umbrella DNS连接器配置

分辨率

故障排除和分析步骤

1：验证FMC是否已完全集成并接收Umbrella DNS策略，以及是否已部署到FTD。

- 确保证书已安装且有效。
- 验证Umbrella令牌和公钥是否配置了解析程序。

- 确保Umbrella策略已应用于FTD，并且Umbrella注册状态显示200 SUCCESS。

<#root>

```
 Firepower# show crypto ca trustpoints

Trustpoint Umbrella_Certificate:
    Subject Name:
    CN=DigiCert TLS RSA SHA256 2020 CA1
    O=DigiCert Inc
    C=US
          Serial Number: 0a3508d55c292b017df8ad65c00ff7e4


 Certificate configured.


firepower# show running-config all umbrella-global
umbrella-global


token ABCDEFGHIJKLMNOP12345678900987654321
 public-key AAAA:BBBB:CCCC:1111:2222:3333:4444:AAAA:BBBB:CCCC:DDDD:1111:2222:3333:4444:5555

 timeout edns 0:02:00
 resolver ipv4 208.67.220.220
 resolver ipv6 2620:119:53::53


firepower# show running-config policy-map type inspect dns
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512


umbrella tag Umbrella_for_FMC_Policy


  no tcp-inspection


firepower# show service-policy inspect dns
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 5982, lock fail 0, drop 1, reset-drop 0, 5-min-pkt-rate 0 pkt
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 2975
        protocol-enforcement, drop 0
        nat-rewrite, count 0

        Umbrella registration: tag: Umbrella_for_FMC_Policy, status: 200 SUCCESS, device-id: 010ac189144
        Umbrella resolver mode: fail-close
        Umbrella resolver ipv4: 208.67.220.220 - operational
        Umbrella resolver ipv6: 2620:119:53::53 - operational
```

```
        Umbrella: bypass 0, req inject 3007 - sent 3007, res recv 3007 - inject 2975, local-domain-bypas

    Class-map: class_snmp
```

2：如果Umbrella注册状态显示Unknown，请使用debugs和show命令验证是否在Umbrella重定向所必需的数据接口上配置了DNS服务器组。

```
firepower# show run dns
firepower# debug umbrella
firepower# debug dns all
firepower# debug ssl 255
```

由于FTD平台设置中的DNS“No interfaces enabled”，FTD-Umbrella在FTD CLI上注册失败，调试的示例：

<#root>

```
firepower# show run dns
DNS server-group DefaultDNS    <== No interfaces enabled
---
Registration Req header: application/json
Host: api.opendns.com
Authorization:OpenDNS,api_key="ABCDEFGHIJKLMNOP1234567890987654321",token="ABCDEFGHIJKLMNOP123456789098
payload: {"model":"9AU9A8XD6QH","macAddress":"deadbeef0000","tag":"DNS_Policy","label":"cisco_NGFWv","na
DNS: get global group DefaultDNS handle 267051f
DNS: Resolve request for 'api.opendns.com' group DefaultDNS

DNS: No interfaces enabled

Response is NULL
odns_cluster_send_device_id_update not ready to send device-id update
odns_ha_send_device_id_update not ready to send device-id update

Registration failed. Retrying...
```

3：更新FTD上的平台设置所需的配置不会再次自动触发Umbrella注册。要强制进行新的注册尝试，请从CLISH提示符重新启动FTD上的DNS检查服务：

<#root>

```
firepower# show run dns

dns domain-lookup outside
dns domain-lookup inside
```

```
DNS server-group DefaultDNS
DNS server-group Umbrella
retries 3
timeout 3
name-server 208.67.220.220
name-server 208.67.222.222
--
Registration Req header: application/json
Host: api.opendns.com
Authorization:OpenDNS,api_key="ABCDEFGHIJKLMNOP1234567890987654321",token="ABCDEFGHIJKLMNOP123456789098
payload: {"model":"9AU9A8XD6QH","macAddress":"deadbeef0000","tag":"DNS_Policy","label":"cisco_NGFWv","na
Response is NULL
odns_cluster_send_device_id_update not ready to send device-id update
odns_ha_send_device_id_update not ready to send device-id update

Registration failed. Retrying...

--
> configure inspection dns disable
> configure inspection dns enable
```

FTD-Umbrella成功注册并调试在FTD CLI上的示例：

<#root>

```
Registration Req header: application/json
Host: api.opendns.com
Authorization:OpenDNS,api_key="09E3D179DF3EC142402CF501361A0BFB",token="1D2ED3B50C59C64C002703447A6B0BF
payload: {"model":"9AU9A8XD6QH","macAddress":"deadbeef0000","tag":"DNS_Policy_Corporate","label":"cisco
DNS: get global group Umbrella handle 4a081ff
DNS: Resolve request for 'api.opendns.com' group Umbrella
dns_cache: Lukup ptr created for thread umbrella_reg,members in lookup_ptr_namelist=1 ,total =1

DNS: Selected interface to send out DNS packet outside

DNS: Message Validated
DNS: Converting Response to DNS Cache Entry

DNS: ** Answer Section **
    AN(0): Name:   api.opendns.com, RR type=1, class=1, ttl=10, datalen=4

DNS: Entry not found in cache, so create one
DNS: namelen 16, txtlen 0
DNS: Reparsing for adding to cache

DNS: hostname is api.opendns.com, RR type=1, class=1, ttl=10, n=4

DNS: Added New Cache Entry
DNS: Added Response to cache

Registration succeeded with deviceID 010a8850c25440ee!

odns_cluster_send_device_id_update not ready to send device-id update
```

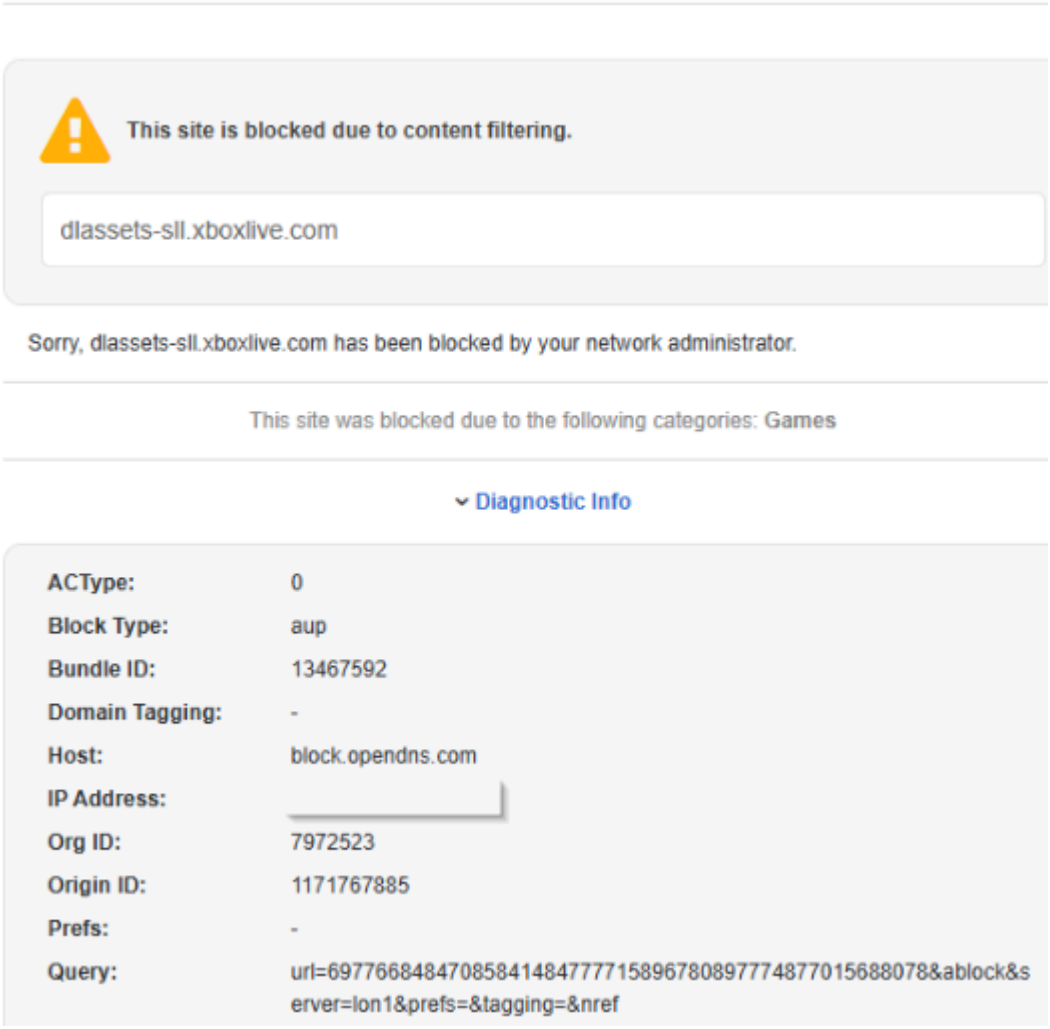
```
odns_ha_send_device_id_update not ready to send device-id update
Registration process exiting...
```

4：使用类似的调试检查FTD DNS检查、注入和重定向到Umbrella。

<#root>

```
Umbrella: DNS REQ map transaction id [0xd77c] to [0x83f0]

Umbrella: modifying REQ [0x83f0] 10.3.0.4 -> 208.67.220.220
Umbrella: adding edns devid: 010a8850c25440ee
Umbrella: modify dst: 208.67.220.220 to 208.67.220.220
dnscrypt_is_ready: CONN inspect 0x0000148f1e216c00, dns_param 0x0000148f1e216c70, flags 2c7, magic_query
Umbrella: inject new REQ [0x83f0] downstream flow handle 9a9b0722
Umbrella: create map_id: [0x83f0] aid_entry: 0x0000148f1e203140

Umbrella: send REQ [0x83f0] 10.3.0.4 -> 208.67.220.220 downstream flow handle 9a9b0722.
snp_fp_dnscrypt: forward flow 10.3.0.4/52952 --> 208.67.220.220/443; inspect 0x0000148f1e213000

dnscrypt_is_ready: CONN inspect 0x0000148f1e213000, dns_param 0x0000148f1e213070, flags 2c7, magic_query
snp_fp_dnscrypt: Received c2s EDNS query pkt from umbrella.
dnscrypt_egress_encrypt: Payload just encrypted.

snp_fp_dnscrypt: Dispatching the packet.
snp_fp_dnscrypt: reverse flow 208.67.220.220/443 --> 192.168.200.245/52952; inspect 0x0000148f1e213000

dnscrypt_is_ready: CONN inspect 0x0000148f1e213000, dns_param 0x0000148f1e213070, flags 2c7, magic_query
snp_fp_dnscrypt: Received u2c in upstream flow; try to decrypt.
dnscrypt_ingress_decrypt: dns udp 0x0000001193282d22 start 0x0000001193282d2a end 0x0000001193282ed7 wp
dnscrypt_ingress_decrypt: new dns_len 397.
dnscrypt_ingress_decrypt: Payload just decrypted; dns_len 173.
dnscrypt_ingress_decrypt: Orig c2s/c2u flow 10.3.0.4/52952 -> 208.67.220.220/443
dnscrypt_ingress_decrypt: Dispatch clear text edns packet
--

Umbrella: recv RES [0x83f0] 192.168.200.245 <- 208.67.220.220

Umbrella: umbrella_pull_tranxn: pull flow (0x0000148f0d6baf68) aid_entry 0x0000148f1e203140 (id=33776/0
Umbrella: umbrella_pull_tranxn: pull found flow (0x0000148f0d6baf68)aid_entry (0x0000148f1e203140) id=3
Umbrella: umbrella_pull_tranxn: Deleting flow (0x0000148f0d6baf68) aid_entry 0x0000148f1e203140 (id=337

Umbrella: modify src: 208.67.220.220 to 208.67.220.220

dnscrypt_is_ready: CONN inspect 0x0000148f1e213000, dns_param 0x0000148f1e213070, flags 2c7, magic_query
Umbrella: restore src port: 53 to 53
Umbrella: modified RES [0x83f0] 192.168.200.245 <- 208.67.220.220

Umbrella: inject new RES [0x83f0]

snp_dbregex_re_get: Getting regexp table 0x00005594320b9f30 for context 0.
umbrella_dbregex_check: matching domain name settings-win.data.microsoft.com (31) against re table 0x00
umbrella_dbregex_check: matched result 0x0000000000000000; matched len 31 regex id 0.
```

5：检查Umbrella仪表板活动日志，以验证FTD流量是否到达Umbrella，以及是否正在对其应用Umbrella策略。最终用户会看到Cisco Umbrella块页面，该页面根据策略配置指示拒绝特定站点类别。



inline_image_0.png

6：更新最终用户DNS配置以直接使用公共DNS服务器而不是OpenDNS/Umbrella解析器。

DNS服务器配置更改示例：

```
Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4
```

原因

客户端虚拟机配置为直接使用OpenDNS/Umbrella解析器而不是标准公共DNS服务器，从而阻止FTD Umbrella DNS连接器的正确DNS重定向和身份属性。当VM明确指向Umbrella DNS服务器时，防火墙无法使用配置的Umbrella组织和策略为客户端正确拦截、插入和转发DNS查询。

预防和建议

- 在依赖FTD Umbrella DNS连接器实施时，确保终端使用标准DNS解析器（内部DNS或公共DNS，如Google DNS）。
- 当预期网络安全设备会进行DNS重定向或注入时，请避免将客户端配置为直接指向Umbrella/OpenDNS解析器。
- 在任何DNS或路由更改后，使用Umbrella活动搜索和策略检查工具验证DNS流量。
- 在部署之前测试生产和实验室环境中的DNS解析行为。

相关内容

- 为Cisco安全防火墙管理中心配置Umbrella DNS连接器
- 为基于令牌的配置续订Umbrella根证书
- 思科技术支持和下载

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）。