使用Umbrella疑難排解FTD註冊問題

目錄

問題

Umbrella網路裝置儀表板顯示思科防火牆管理中心(FMC)已整合和連線。FMC還可以將Umbrella策略拉到FMC並將其部署到思科防火牆威脅防禦(FTD)。但是，FTD無法註冊到Umbrella以重定向DNS流量。

環境

- Cisco安全防火牆Firepower FTD 10.0.0（適用於7.2+版）
- 防火牆管理中心(FMC)版本10.0.0（適用於7.2+版）
- 在Azure虛擬WAN環境中部署（也適用於硬體模型）
- FMC已成功與思科資安防護林相整合
- FTD上的Umbrella DNS聯結器組態

解析

故障排除和分析步驟

1：驗證FMC是否已完全整合並接收Umbrella DNS策略，以及是否已部署到FTD。

- 確保證書已安裝並且有效。
- 驗證Umbrella令牌和公鑰是否配置了解析程式。

- 確保Umbrella原則已套用到FTD，而Umbrella註冊狀態顯示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註冊狀態顯示Unknown，請使用debugs和show命令來驗證是否在Umbrella重定向所必需的資料介面上配置了DNS伺服器組。

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

由於FTD平台設定中DNS的「No interfaces enabled」，導致FTD-Umbrella註冊失敗，在FTD CLI上偵錯的範例：

<#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上的平台設定所需的配置不會再次自動觸發Umbrella註冊。若要強制進行新的註冊嘗試，請從CLISH提示符重新啟動FTD上的DNS檢查服務：

<#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
```

成功在FTD CLI上使用偵錯進行FTD-Umbrella註冊的範例：

<#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
```

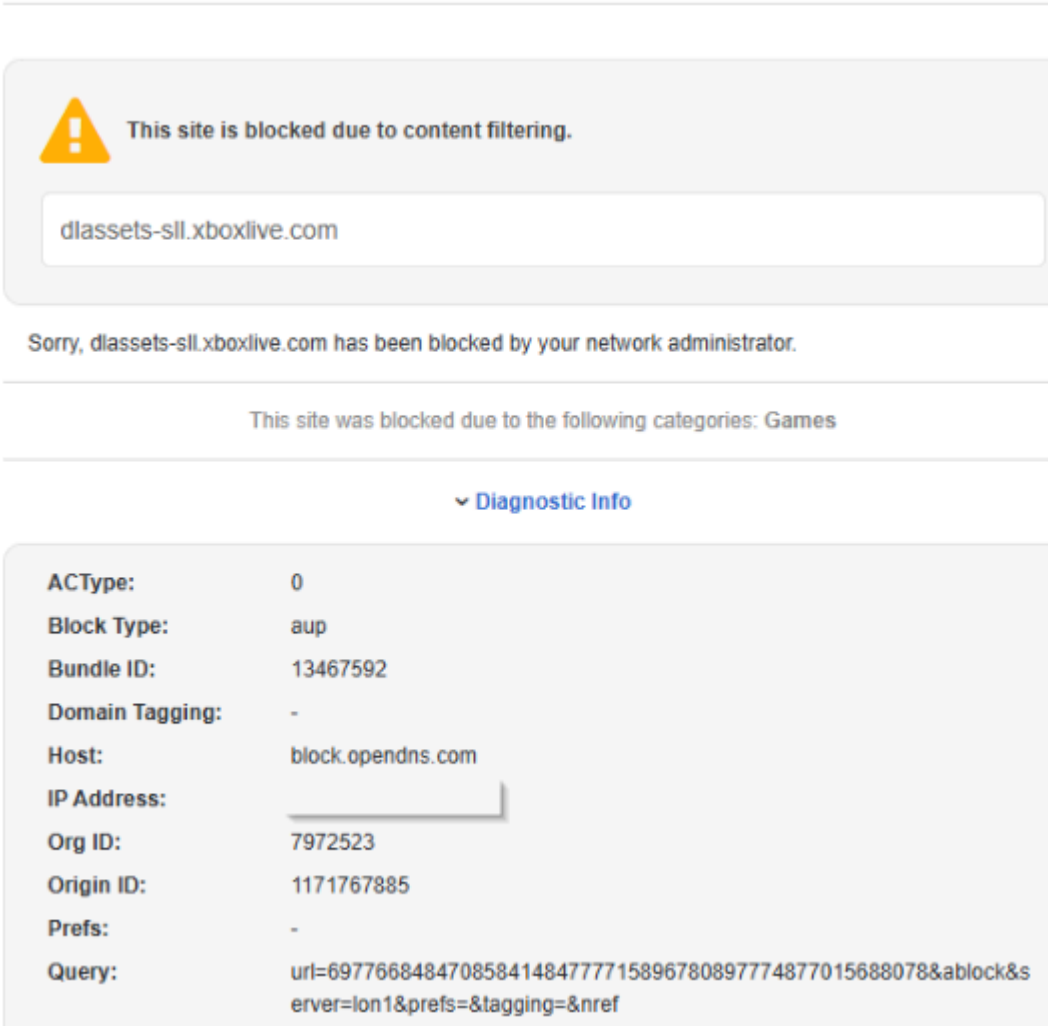
```
odns_ha_send_device_id_update not ready to send device-id update
Registration process exiting...
```

4：使用類似的調試檢視FTD DNS檢查、注入和重定向至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：檢查Umbrella儀表板活動日誌，以驗證FTD流量是否到達Umbrella，以及是否正在對其應用Umbrella策略。終端使用者會看到Cisco Umbrella塊頁面，該頁面根據策略配置指示拒絕特定站點類別。



inline_image_0.png

6：更新終端使用者DNS配置以直接使用公共DNS伺服器而不是OpenDNS/Umbrella解析程式。

DNS伺服器配置更改示例：

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

原因

已將客戶端虛擬機器配置為直接使用OpenDNS/Umbrella解析器而不是標準公共DNS伺服器，從而阻止FTD Umbrella DNS聯結器進行正確的DNS重定向和身份屬性。當VM明確指向Umbrella DNS伺服器時，防火牆無法使用配置的Umbrella組織和策略代表客戶端正確攔截、插入和轉發DNS查詢。

預防措施和建議

- 在依賴FTD Umbrella DNS聯結器執行時，確保終端使用標準DNS解析器（內部DNS或公共DNS，例如Google DNS）。
- 避免將客戶端配置為在預期從網路安全裝置進行DNS重定向或注入時直接指向Umbrella/OpenDNS解析器。
- 在任何DNS或路由更改後，使用Umbrella活動搜尋和策略檢查器工具驗證DNS流。
- 在部署之前測試生產和實驗室環境中的DNS解析行為。

相關內容

- 為Cisco安全防火牆管理中心配置Umbrella DNS聯結器
- 續訂基於令牌的配置的Umbrella根證書
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。