Umbrellaを使用したFTD登録問題のトラブルシューティング

内容

お問い合わせ内容

Umbrella Network Devicesダッシュボードには、Cisco Firewall Management Center(FMC)がすでに統合および接続されていることが表示されます。 また、FMCは包括ポリシーをFMCにプルし、シスコファイアウォール脅威対策(FTD)に展開することもできます。 ただし、FTDはUmbrellaに登録してDNSトラフィックをリダイレクトすることができません。

環境

- Cisco Secure Firewall Firepower FTD 10.0.0（バージョン7.2以降に適用可能）
- Firewall Management Center(FMC)バージョン10.0.0（バージョン7.2以降に適用可能）
- Azure Virtual WAN環境での配置（ハードウェアモデルにも適用可能）
- FMCはCisco Umbrellaと正常に統合
- FTDでのUmbrella DNSコネクタの設定

解決策

トラブルシューティングと分析の手順

1: FMCが完全に統合され、Umbrella DNSポリシーを受信していること、およびこれらがFTDに展開されていることを確認します。

- 証明書がインストールされ、有効であることを確認します。
- Umbrellaトークンと公開キーに設定されているリゾルバがあることを確認します。
- UmbrellaポリシーがFTDに適用されており、Umbrella登録ステータスが200 SUCCESSを示していることを確認します。

<#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 ABCDEFGHIJKLMNOP12345678909876543 21
 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: Umbrella登録のステータスにUnknownが表示された場合は、デバッグとshowコマンドを使用して、DNSサーバグループがUmbrellaリダイレクションに必要なデータインターフェイスに設定されていることを検証します。

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

FTDプラットフォーム設定でDNSに対して「インターフェイスが有効になっていません」ことが原因でFTD CLIでデバッグを行い、FTD-Umbrella登録に失敗した例：

<#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:FTDのプラットフォーム設定に必要な設定を更新しても、Umbrella登録が自動的に再びトリガーされることはありません。 新しい登録を強制的に試行するには、CLISHプロンプトからFTDでDNSインスペクションサービスを再起動します。

<#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="ABCDEFGHIJKLMNOP12345678909876543 21",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 CLIでデバッグを行い、FTD-Umbrellaを正常に登録した例を次に示します。

<#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...
```

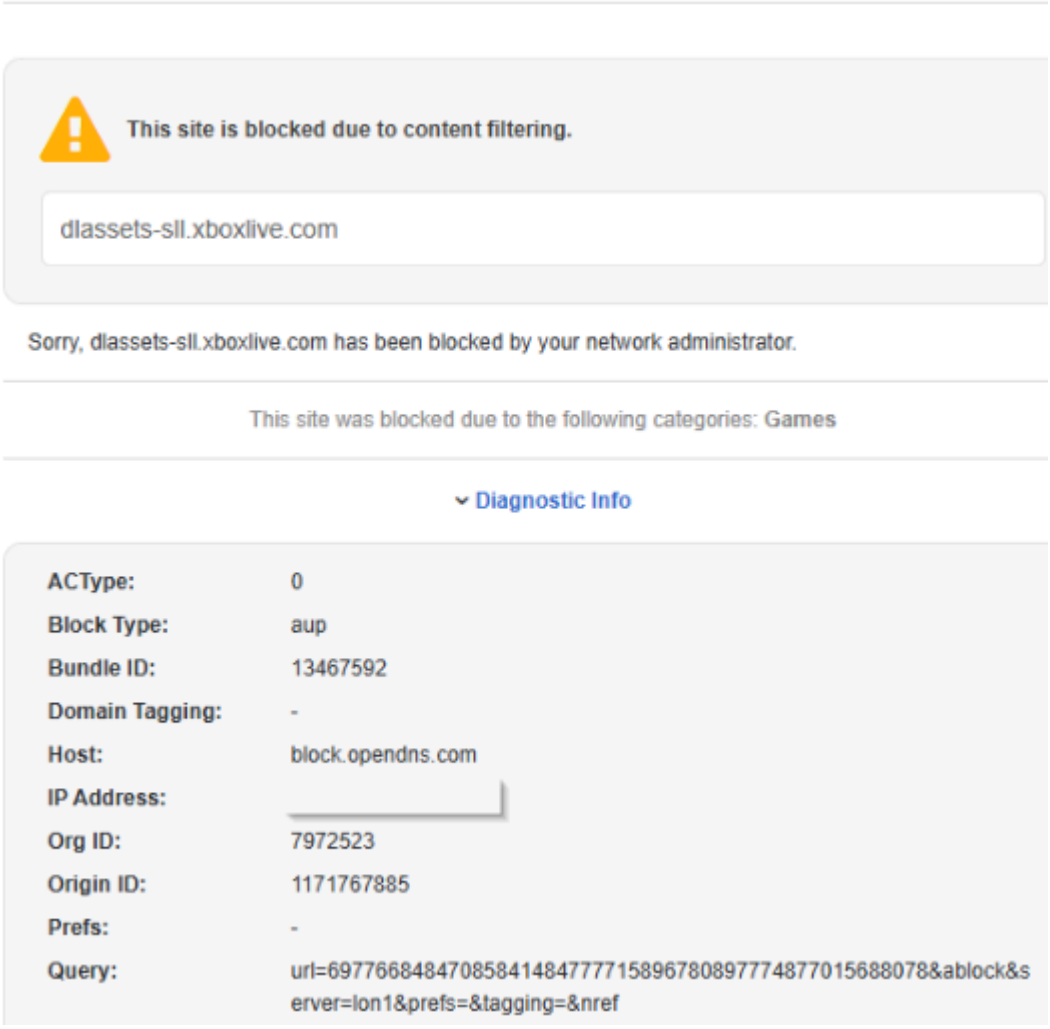
4：同様のデバッグを使用して、FTD DNSインスペクション、インジェクション、および Umbrellaへのリダイレクションを確認します。

<#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:Umbrellaダッシュボードのアクティビティログをチェックして、FTDトラフィックがUmbrellaに到達していること、およびUmbrellaポリシーが適用されていることを確認します。 エンドユーザには、ポリシー設定に基づいて特定のサイトカテゴリへの拒否を示すCisco Umbrellaブロックページが表示されます。



inline_image_0.png (インラインイメージ_0.png)

6:OpenDNS/Umbrellaリゾルバを直接使用する代わりにパブリックDNSサーバを使用するように、エンドユーザのDNS設定を更新します。

DNSサーバ設定の変更例：

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

原因

クライアント仮想マシンは、標準のパブリックDNSサーバの代わりにOpenDNS/Umbrellaリゾルバを直接使用するように設定され、FTD Umbrella DNSコネクタによる適切なDNSリダイレクションとID帰属を防止していました。 VMがUmbrella DNSサーバを明示的に指している場合、ファイアウォールは、設定されたUmbrella組織とポリシーを使用して、クライアントに代わってDNSクエリを正しく代行受信、挿入、転送できません。

予防と推奨事項

- FTD Umbrella DNSコネクタに依存して適用する場合、エンドポイントが標準のDNSリゾルバ（内部DNSまたはGoogle DNSなどのパブリックDNS）を使用していることを確認します。
- ネットワークセキュリティデバイスからDNSリダイレクトまたはインジェクションが期待される場合は、Umbrella/OpenDNSリゾルバを直接ポイントするようにクライアントを設定することは避けてください。
- DNSまたはルーティングの変更後、Umbrellaアクティビティ検索ツールおよびポリシーチェッカーツールを使用してDNSフローを検証します。
- 実稼働環境とラボ環境の両方で、導入前にDNS解決動作をテストします。

関連コンテンツ

- Cisco Secure Firewall Management Center用のUmbrella DNSコネクタの設定
- トークンベースの構成の包括ルート証明書の更新
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。