Umbrella를 사용하여 FTD 등록 문제 해결

목차

문제

Umbrella Network Devices 대시보드에는 이미 통합 및 연결된 Cisco FMC(Firewall Management Center)가 표시됩니다. 또한 FMC는 FMC에 Umbrella 정책을 가져와 Cisco FTD(Firewall Threat Defense)에 배포할 수 있습니다. 그러나 FTD는 DNS 트래픽을 리디렉션하기 위해 Umbrella에 등록할 수 없습니다.

환경

- Cisco Secure Firewall Firepower FTD 10.0.0(버전 7.2 이상에 적용 가능)
- FMC(Firewall Management Center) 버전 10.0.0(버전 7.2 이상에 적용 가능)
- Azure 가상 WAN 환경에서 배포(하드웨어 모델에도 적용 가능)
- FMC가 Cisco Umbrella와 성공적으로 통합
- FTD의 Umbrella DNS Connector 컨피그레이션

해결

문제 해결 및 분석 단계

1: FMC가 완전히 통합되어 있고 Umbrella DNS 정책을 수신하고 있으며 FTD에 구축되어 있는지 확인합니다.

- 인증서가 설치되어 있고 유효한지 확인하십시오.
- Umbrella 토큰 및 공개 키가 구성된 확인자와 함께 있는지 확인합니다.
- Umbrella 정책이 FTD에 적용되었는지 확인하고 Umbrella 등록 상태는 200 SUCCESS를 표시합니다.

<#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 등록 상태가 Unknown(알 수 없음)으로 표시되면 debugs 및 show 명령을 사용하여 Umbrella 리디렉션에 필요한 데이터 인터페이스에 DNS 서버 그룹이 구성되었는지 확인합니다.

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

FTD 플랫폼 설정에서 DNS에 대해 "활성화된 인터페이스 없음"으로 인해 FTD CLI에서 디버그를 사용한 실패한 FTD-Umbrella 등록의 예:

<#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: FTD에서 플랫폼 설정에 필요한 구성을 업데이트해도 Umbrella 등록이 자동으로 다시 트리거되지 않습니다. 새 등록을 강제로 시도하려면 CLISH 프롬프트에서 FTD에서 DNS 검사 서비스를 다시 시작하십시오.

<#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 CLI에서 디버그를 사용한 성공적인 FTD-Umbrella 등록의 예:

<#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...
```

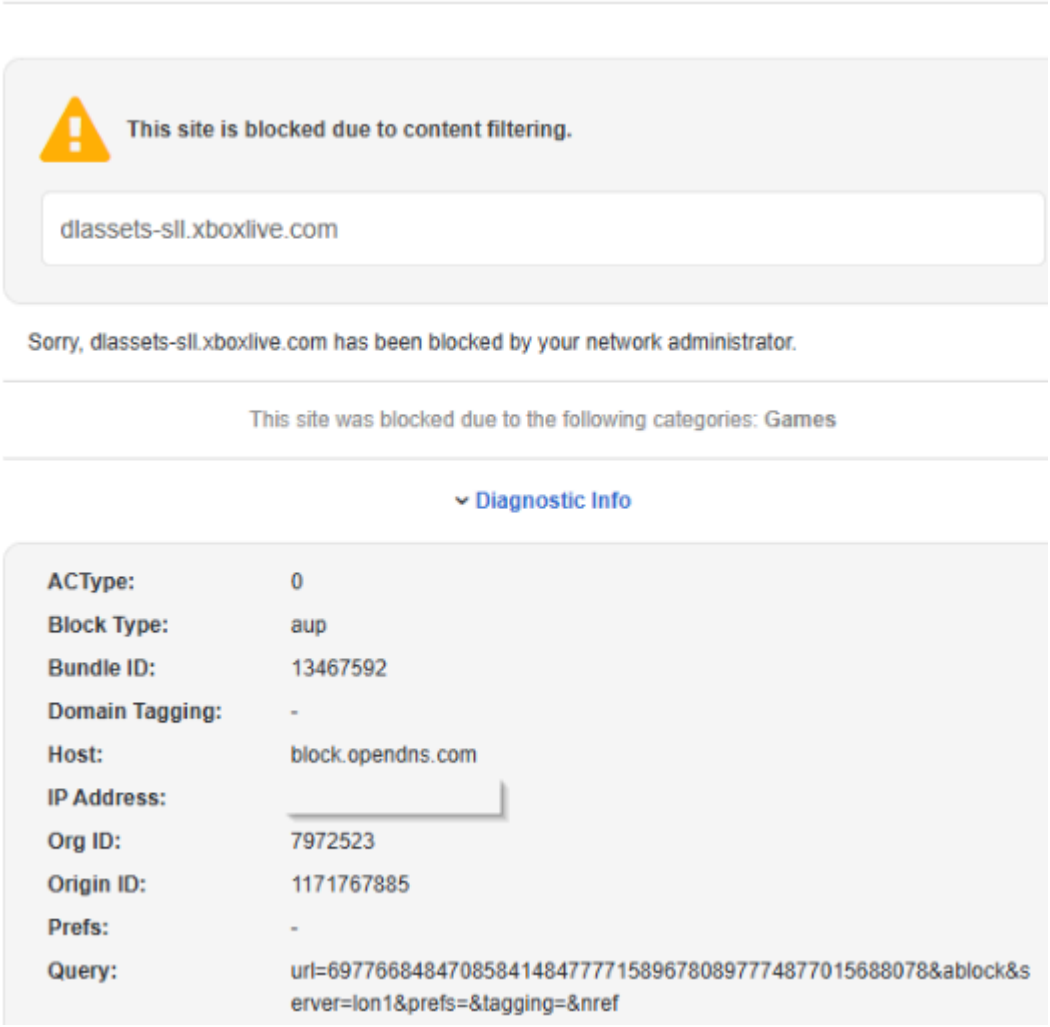
4: 유사한 디버그를 사용하여 FTD DNS 검사, 주입 및 Umbrella로의 리디렉션을 검토합니다.

<#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 대시보드 작업 로그를 확인하여 FTD 트래픽이 Umbrella에 도달하고 Umbrella 정책이 적용되는지 확인합니다. 최종 사용자는 정책 구성에 따라 특정 사이트 범주에 대한 거부를 나타내는 Cisco Umbrella 블록 페이지를 볼 수 있습니다.



inline_image_0.png

6: OpenDNS/Umbrella 확인자 대신 공용 DNS 서버를 직접 사용하도록 최종 사용자 DNS 컨피그레이션을 업데이트합니다.

DNS 서버 컨피그레이션 변경 예:

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

원인

클라이언트 가상 컴퓨터가 표준 공용 DNS 서버 대신 OpenDNS/Umbrella 리졸버를 직접 사용하도록 구성되어 있어 FTD Umbrella DNS 커넥터가 DNS 리디렉션 및 ID 특성을 제대로 지정할 수 없습니다. VM이 Umbrella DNS 서버를 명시적으로 가리키면 방화벽이 구성된 Umbrella 조직 및 정책을 사용하여 클라이언트 대신 DNS 쿼리를 올바르게 가로채고, 삽입하고, 전달할 수 없습니다.

예방 및 권장 사항

- 시행을 위해 FTD Umbrella DNS Connector에 의존할 때 엔드포인트가 표준 DNS 리졸버(내부 DNS 또는 Google DNS와 같은 공용 DNS)를 사용하도록 합니다.
- 네트워크 보안 디바이스에서 DNS 리디렉션 또는 삽입이 예상되는 경우 클라이언트가 Umbrella/OpenDNS 리졸버를 직접 가리키도록 구성하지 마십시오.
- DNS 또는 라우팅 변경 후 Umbrella 활동 검색 및 정책 검사기 툴을 사용하여 DNS 흐름을 검증합니다.
- 구축 전에 프로덕션 및 랩 환경 모두에서 DNS 확인 동작을 테스트합니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center용 Umbrella DNS 커넥터 구성
- 토큰 기반 컨피그레이션을 위한 Umbrella 루트 인증서 갱신
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.