أستكشاف أخطاء تسجيل FTD وإصلاحها مع Umbrella

المحتويات

مسألة

توضح هذه المقالة كيفية أستكشاف أخطاء تسجيل FTD وإصلاحها مع Umbrella.

البيئة

- Cisco Secure Firewall Firepower FTD 10.0.0 (قابل للتطبيق على الإصدارات 7.2+)
- مركز إدارة جدران الحماية (FMC) الإصدار 10.0.0 (قابل للتطبيق على الإصدارات 7.2+)
- النشر في بيئة شبكة WAN الظاهرية من Azure (قابلة للتطبيق على طرز الأجهزة أيضا)
- تم دمج FMC بنجاح مع Cisco Umbrella
- تكوين موصل DNS Umbrella على FTD

قرار

خطوات أستكشاف الأخطاء وإصلاحها والتحليل

1: التحقق من أن FMC مدمج بالكامل وتتلقى سياسات DNS Umbrella ومن أنها قد تم نشرها

في "برنامج الإرسال فائق السرعة".

- تأكد من تثبيت الشهادة وصلاحيتها.
- تحقق من أن رمز Umbrella المميز والمفاتيح العامة تم تكوينها بواسطة المحددات.
- تأكد من تطبيق سياسة Umbrella على FTD وتظهر حالة التسجيل في Umbrella نجاح 200.

<#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 ABCDEFGHIJKLMNOP1234567890987654321
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: إذا كانت حالة تسجيل Umbrella تظهر غير معروف، فاستخدم أوامر تصحيح الأخطاء وshow للتحقق من تكوين مجموعة خوادم DNS على واجهات البيانات الضرورية لإعادة توجيه حركة مرور Umbrella.

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

مثال على فشل تسجيل FTD-Umbrella مع تصحيح الأخطاء على FTD CLI بسبب "عدم تكوين واجهات" لـ DNS في إعدادات النظام الأساسي لـ FTD:

<#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: إلى أيقاف تلقائي FTD على النظام الأساسي لإعدادات اللازمة لتكوينات التي تؤدي تحديث ال تشغيل تسجيل Umbrella مرة أخرى. لفرض محاولة تسجيل جديدة، قم بإعادة تشغيل خدمة

فحص DNS على FTD من المطالبة CLISH:

```
<#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
```

مثال على التسجيل الناجح في FTD-Umbrella مع تصحيح الأخطاء على واجهة سطر الأوامر FTD (CLI):

```
<#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: مراجعة فحص FTD DNS والحقن وإعادة التوجيه إلى Umbrella باستخدام تصحيح أخطاء مماثل.

<#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
```

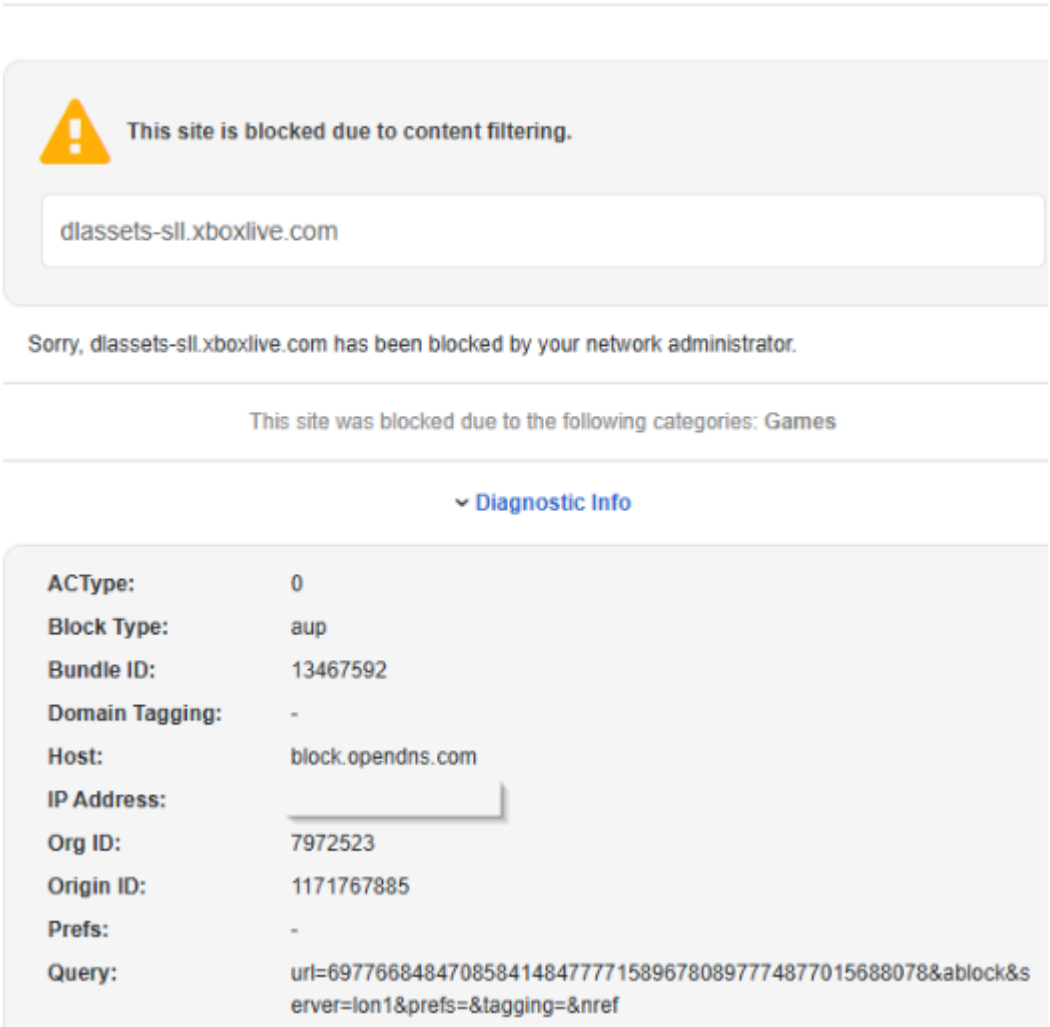
```
                                        Umbrella: modify src: 208.67.220.220 to 208.67.220.220

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: تحقق من سجلات Umbrella Dashboard Activity للتحقق من وصول حركة مرور بيانات FTD إلى Umbrella ومن تطبيق سياسات Umbrella عليها. يرى المستخدمون النهائيون صفحة Cisco Umbrella Block تشير إلى رفض فئات موقع معينة، استنادا إلى تكوينات النهج.



inline_image_0.png

6: تحديث تكوين DNS للمستخدم النهائي لاستخدام خوادم DNS العامة بدلا من محولات OpenDNS/Umbrella مباشرة.

مثال على تغيير تكوين خادم DNS:

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

السبب

تم تكوين الأجهزة الظاهرية للعملاء لاستخدام محولات OpenDNS/Umbrella مباشرة بدلا من خوادم DNS العامة القياسية، مما يمنع إعادة توجيه DNS بشكل مناسب وتخصيص الهوية بشكل صريح VMs. عندما تشير FTD Umbrella في تكوين DNS الذي تم توصيل DNS من قبل إلى خوادم Umbrella DNS، لا يمكن لجدار الحماية اعتراض استعلامات DNS وحفظها وإعادة توجيهها بشكل صحيح نيابة عن العملاء باستخدام مؤسسة Umbrella والنهج اللذين تم تكوينهما.

ألف - الوقاية والتوصيات

- تأكد من إستخدام نقاط النهاية لمحددات DNS القياسية (DNS الداخلي أو DNS العامة) للإنفاذ. FTD Umbrella الخاص ب DNS توصيل على الاعتماد عند (Google DNS مثل)
- تجنب تكوين العملاء للإشارة مباشرة إلى وحدات تحليل Umbrella/OpenDNS عند توقع إعادة توجيه DNS أو حقن من أجهزة أمان الشبكة.
- تحقق من تدفق DNS باستخدام أدوات البحث عن نشاط Umbrella وأدوات مدقق النهج بعد أي تغييرات في DNS أو التوجيه.
- قم باختبار سلوك تحليل DNS في كل من بيئات الإنتاج والمختبرات قبل النشر.

المحتوى ذي الصلة

- [تكوين موصل DNS الظلي لمركز إدارة جدار الحماية الآمن من Cisco](#)
- [تجديد شهادة جذر الظلة للتكوين المستند إلى الرمز المميز](#)
- [الدعم الفني والتنزيلات من Cisco](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).