Problemen met FTD-registratie oplossen met paraplu

Inhoud

uitgeven

Het dashboard van Umbrella Network Devices toont het Cisco Firewall Management Center (FMC) dat al is geïntegreerd en verbonden. De FMC is ook in staat om het overkoepelende beleid naar de FMC te trekken en deze in te zetten voor de Cisco Firewall Threat Defense (FTD). De FTD kan zich echter niet registreren bij Umbrella om DNS-verkeer om te leiden.

milieu

- Cisco Secure Firewall Firepower FTD 10.0.0 (van toepassing op versies 7.2+)
- Firewall Management Center (FMC) versie 10.0.0 (van toepassing op versies 7.2+)
- Implementatie in Azure Virtual WAN-omgeving (ook van toepassing op hardwaremodellen)
- FMC succesvol geïntegreerd met Cisco Umbrella
- Umbrella DNS Connector configuratie op FTD

resolutie

Stappen voor probleemoplossing en analyse

1: Controleer of het VCC volledig geïntegreerd is en een overkoepelend DNS-beleid ontvangt en of het wordt ingezet voor het FTD.

- Controleer of het certificaat is geïnstalleerd en geldig is.
- Valideer dat de Umbrella-token en publieke sleutel zijn geconfigureerd met resolvers.
- Ervoor zorgen dat het overkoepelende beleid is toegepast op het FTD en dat de overkoepelende registratiestatus 200 SUCCES laat zien.

<#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: Als de registratiestatus van de paraplu Onbekend toont, gebruikt u foutopsporing en toont u opdrachten om te valideren dat een DNS-servergroep is geconfigureerd op de benodigde gegevensinterfaces voor omleiding van de paraplu.

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

Voorbeeld van mislukte FTD-Umbrella-registratie met fouten op FTD CLI vanwege "Geen interfaces ingeschakeld" voor DNS in FTD-platforminstellingen:

<#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: Het updaten van de benodigde configuraties voor platforminstellingen op de FTD leidt niet automatisch tot een nieuwe registratie van de paraplu. Als u een nieuwe registratiepoging wilt forceren, start u de DNS-inspectiedienst op de FTD opnieuw op vanaf de CLISH-prompt:

<#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
```

Voorbeeld van succesvolle FTD-Umbrella registratie met debugs op 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: Controleer FTD DNS-inspectie, injectie en omleiding naar Umbrella met behulp van vergelijkbare debugs.

<#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

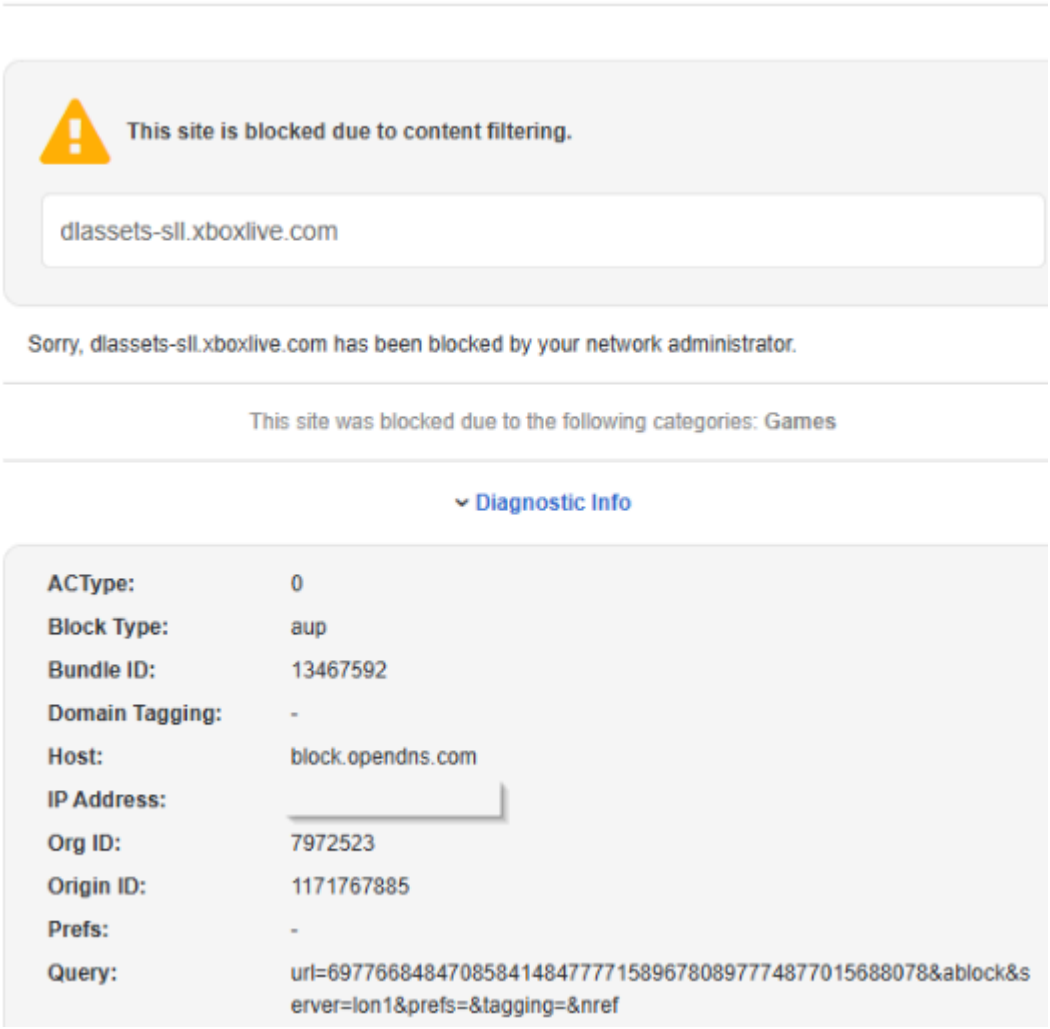
```
dnscrypt_is_ready: CONN inspect 0x0000148f1e213000, dns_param 0x0000148f1e213070, flags 2c7, magic_query
Umbrella: restore src port: 53 to 53
```

```
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: Controleer de activiteitenlogboeken van het Umbrella-dashboard om te controleren of het FTD-verkeer de Umbrella bereikt en of het Umbrella-beleid erop wordt toegepast. Eindgebruikers zien een Cisco Umbrella-blokpagina die de weigering van specifieke sitecategorieën aangeeft, op basis van beleidsconfiguraties.



inline_image_0.png

6: Update de DNS-configuratie van de eindgebruiker om openbare DNS-servers te gebruiken in plaats van OpenDNS/Umbrella Resolvers rechtstreeks.

Voorbeeld wijziging configuratie DNS-server:

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

Oorzaak

Client virtuele machines werden geconfigureerd om OpenDNS/Umbrella resolvers direct te gebruiken in plaats van standaard publieke DNS-servers, waardoor de juiste DNS-omleiding en identiteitstoekenning door de FTD Umbrella DNS Connector werd voorkomen. Wanneer VM's expliciet naar Umbrella DNS-servers verwijzen, kan de firewall DNS-query's niet correct onderscheppen, injecteren en doorsturen namens de clients die de geconfigureerde Umbrella-organisatie en het beleid gebruiken.

Preventie en aanbevelingen

- Zorg ervoor dat eindpunten standaard DNS-resolvers (interne DNS of openbare DNS zoals Google DNS) gebruiken wanneer ze vertrouwen op de FTD Umbrella DNS Connector voor handhaving.
- Vermijd het configureren van clients om direct naar Umbrella/OpenDNS-resolvers te verwijzen wanneer DNS-omleiding of -injectie wordt verwacht van netwerkbeveiligingsapparaten.
- Valideer DNS-stroom met behulp van Umbrella activity search en policy checker tools na eventuele DNS- of routeringswijzigingen.
- Test het DNS-resolutiegedrag in zowel productie- als laboratoriumomgevingen voordat het wordt geïmplementeerd.

Verwante inhoud

- De overkoepelende DNS-connector configureren voor het Cisco Secure Firewall Management Center
- Umbrella Root Certificate vernieuwen voor token-gebaseerde configuratie
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.