Risoluzione dei problemi di registrazione FTD con Umbrella

Sommario

Problema

Nel dashboard Periferiche di rete Umbrella è visualizzato il Cisco Firewall Management Center (FMC) già integrato e connesso. Il FMC è inoltre in grado di recuperare i criteri Umbrella dal FMC e distribuirli al Cisco Firewall Threat Defense (FTD). Tuttavia, il FTD non è in grado di registrarsi in Umbrella per reindirizzare il traffico DNS.

Ambiente

- Cisco Secure Firewall Firepower FTD 10.0.0 (applicabile alle versioni 7.2+)
- Firewall Management Center (FMC) versione 10.0.0 (applicabile alle versioni 7.2+)
- Distribuzione nell'ambiente Virtual WAN di Azure (applicabile anche ai modelli hardware)
- Integrazione di FMC con Cisco Umbrella completata
- Configurazione Umbrella DNS Connector su FTD

Risoluzione

Fasi di risoluzione dei problemi e analisi

1: Verificare che il CCP sia completamente integrato e riceva i criteri DNS ombrello e che siano distribuiti nel FTD.

- Verificare che il certificato sia installato e valido.
- Verificare che il token Umbrella e la chiave pubblica siano configurati con i resolver.
- Verificare che il criterio Umbrella sia stato applicato all'FTD e che lo stato di registrazione Umbrella sia 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 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: se lo stato della registrazione Umbrella indica Sconosciuto, utilizzare i debug e i comandi show per verificare che un gruppo di server DNS sia configurato sulle interfacce dati necessarie per il reindirizzamento Umbrella.

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

Esempio di registrazione FTD-Umbrella non riuscita con debug sulla CLI FTD a causa di "Nessuna interfaccia abilitata" per DNS nelle impostazioni della piattaforma 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: L'aggiornamento delle configurazioni necessarie per le impostazioni della piattaforma sull'FTD non attiva automaticamente di nuovo la registrazione Umbrella. Per forzare un nuovo tentativo di registrazione, riavviare il servizio di ispezione DNS sull'FTD dal prompt 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="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
```

Esempio di registrazione FTD-Umbrella riuscita con debug sulla CLI FTD:

<#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...
```

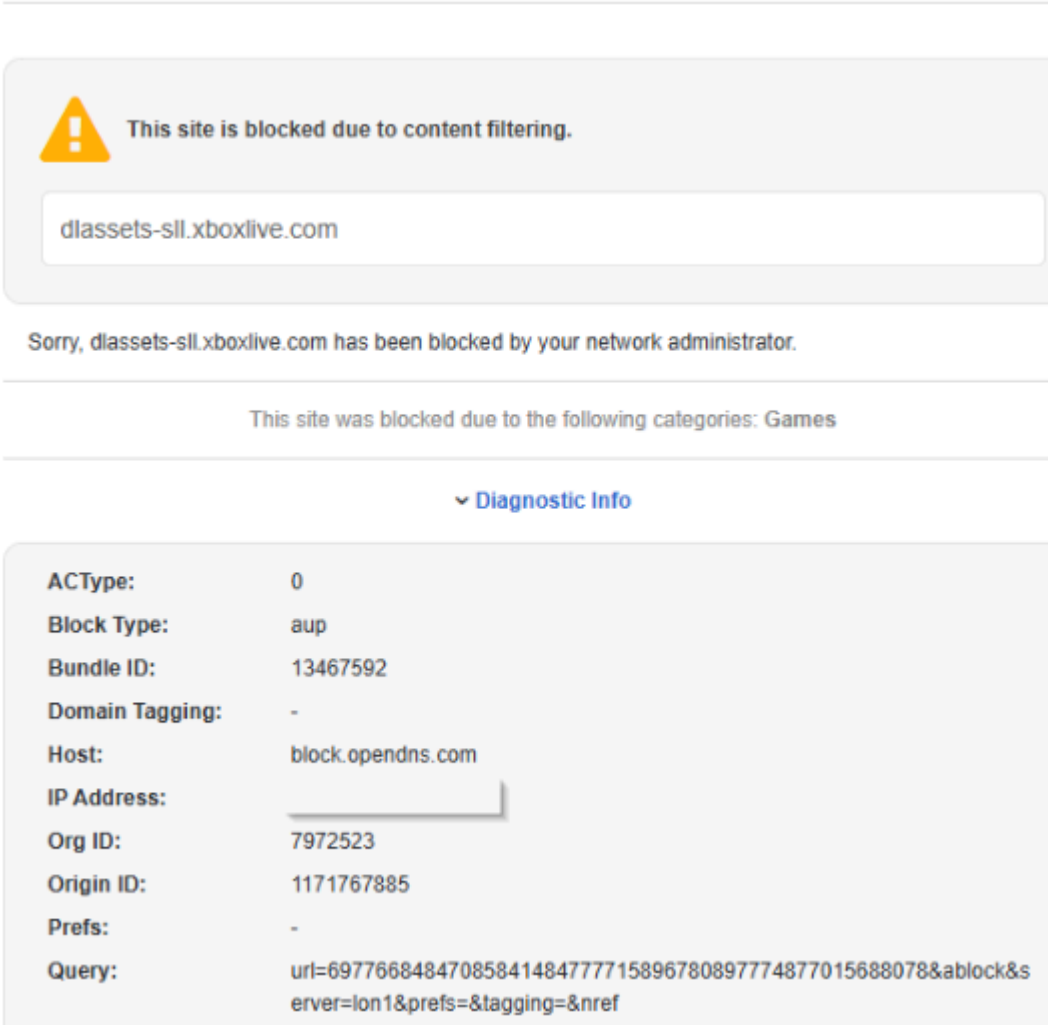
4: Esaminare l'ispezione, l'inserimento e il reindirizzamento del DNS FTD a Umbrella utilizzando debug simili.

<#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: controllare i log attività del dashboard Umbrella per verificare che il traffico FTD raggiunga Umbrella e che i relativi criteri Umbrella siano applicati. Gli utenti finali visualizzano una pagina blocco Cisco Umbrella che indica il rifiuto di accesso a categorie di siti specifiche, in base alle configurazioni dei criteri.



inline_image_0.png

6: Aggiornare la configurazione del DNS dell'utente finale per utilizzare direttamente i server DNS pubblici anziché i resolver OpenDNS/Umbrella.

Esempio di modifica della configurazione del server DNS:

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

Causa

Le macchine virtuali client sono state configurate per utilizzare i resolver OpenDNS/Umbrella direttamente anziché i server DNS pubblici standard, impedendo il reindirizzamento DNS corretto e l'attribuzione di identità da parte del connettore DNS Umbrella FTD. Quando le macchine virtuali puntano esplicitamente ai server DNS Umbrella, il firewall non può intercettare, inserire e inoltrare correttamente query DNS per conto dei client che utilizzano l'organizzazione e i criteri Umbrella configurati.

Prevenzione e raccomandazioni

- Assicurarsi che gli endpoint utilizzino i resolver DNS standard (DNS interno o pubblico, ad esempio Google DNS) quando si basano sul connettore DNS Umbrella FTD per l'imposizione.
- Evitare di configurare i client in modo che puntino direttamente ai resolver Umbrella/OpenDNS quando è previsto il reindirizzamento o l'inserimento DNS da dispositivi di sicurezza di rete.
- Convalidare il flusso DNS utilizzando gli strumenti di controllo criteri e ricerca attività Umbrella dopo qualsiasi modifica del DNS o del routing.
- Verificare il comportamento della risoluzione DNS in ambienti di produzione e di laboratorio prima della distribuzione.

Contenuto correlato

- Configurazione del connettore DNS Umbrella per Cisco Secure Firewall Management Center
- Rinnova certificato radice Umbrella per configurazione basata su token
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).