Résolution des problèmes d'enregistrement FTD avec Umbrella

Table des matières

Problème

Le tableau de bord Périphériques réseau Umbrella affiche le Cisco Firewall Management Center (FMC) déjà intégré et connecté. Le FMC peut également extraire des politiques Umbrella vers le FMC et les déployer vers Cisco Firewall Threat Defense (FTD). Cependant, le FMC ne peut pas s'enregistrer auprès d'Umbrella pour rediriger le trafic DNS.

Environnement

- Cisco Secure Firewall Firepower FTD 10.0.0 (applicable aux versions 7.2 et ultérieures)
- Firewall Management Center (FMC) version 10.0.0 (applicable aux versions 7.2 et ultérieures)
- Déploiement dans l'environnement WAN virtuel Azure (applicable également aux modèles matériels)
- Intégration réussie de FMC à Cisco Umbrella
- Configuration du connecteur DNS de parapluie sur FTD

Résolution

Étapes de dépannage et d'analyse

1 : vérifiez que le FMC est entièrement intégré et qu'il reçoit les politiques de DNS-cadre et qu'elles sont déployées sur le FTD.

- Assurez-vous que le certificat est installé et valide.
- Vérifiez que le jeton Umbrella et la clé publique sont configurés avec des résolveurs.
- Assurez-vous que la politique Umbrella a été appliquée au FTD et que l'état d'enregistrement Umbrella indique 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 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 : Si l'état d'enregistrement Umbrella indique Unknown, utilisez les commandes debugs et show pour valider qu'un groupe de serveurs DNS est configuré sur les interfaces de données nécessaires pour la redirection Umbrella.

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

Exemple d'échec de l'enregistrement FTD-Umbrella avec des débogages sur l'interface de ligne de commande FTD en raison de l'absence d'interfaces activées pour DNS dans les paramètres de la plate-forme 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 : La mise à jour des configurations nécessaires pour les paramètres de plate-forme sur le FTD ne déclenche pas automatiquement à nouveau l'enregistrement Umbrella. Pour forcer une nouvelle tentative d'enregistrement, redémarrez le service d'inspection DNS sur le FTD à partir de l'invite 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
```

Exemple d'enregistrement FTD-Umbrella réussi avec des débogages sur l'interface de ligne de commande 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 : Examinez l'inspection, l'injection et la redirection DNS FTD vers Umbrella à l'aide de débogages similaires.

<#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
```

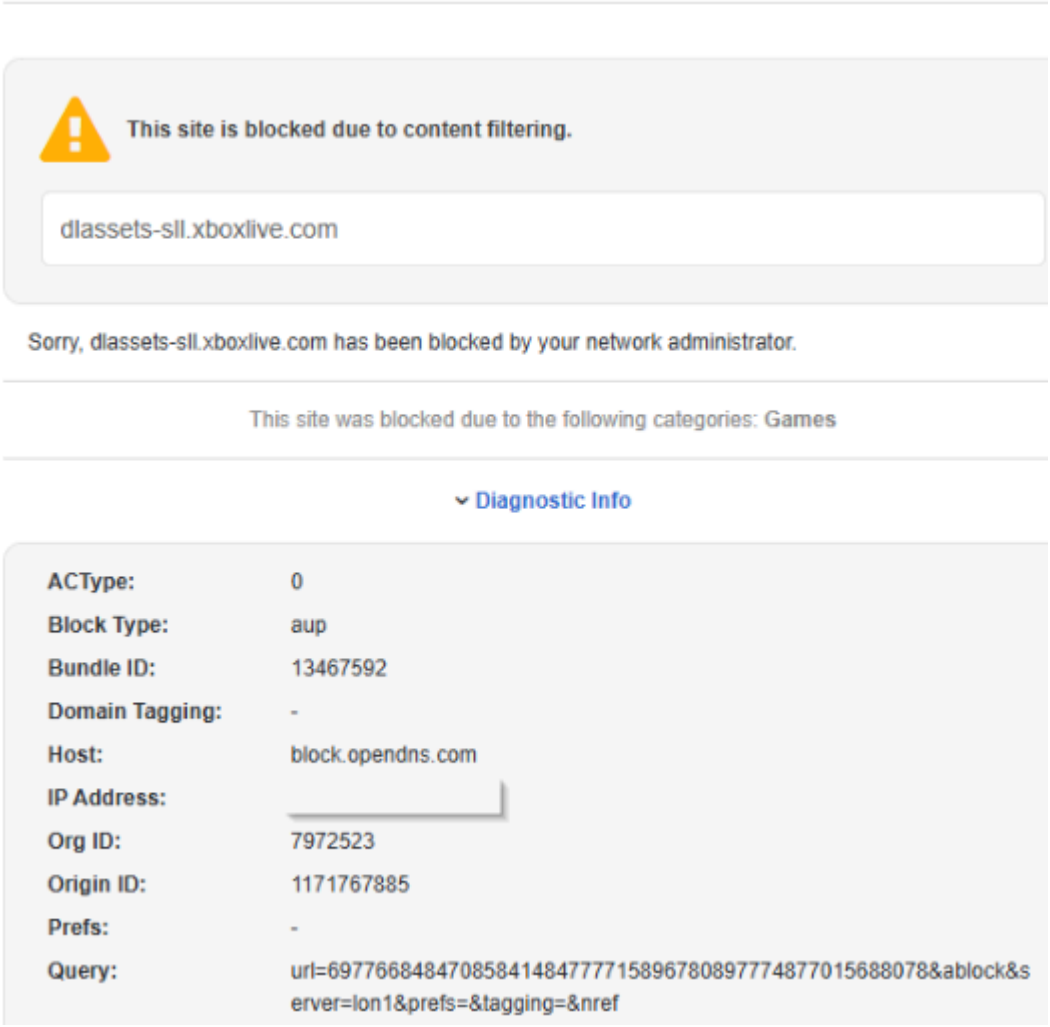
`Umbrella: modify src: 208.67.220.220 to 208.67.220.220`

```
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 : Consultez les journaux d'activité du tableau de bord Umbrella pour vérifier que le trafic FTD atteint Umbrella et que les politiques Umbrella lui sont appliquées. Les utilisateurs finaux voient une page de blocage Cisco Umbrella indiquant un refus à des catégories de sites spécifiques, en fonction des configurations de politiques.



image_en_ligne_0.png

6 : Mettez à jour la configuration DNS de l'utilisateur final pour utiliser directement les serveurs DNS publics au lieu des résolveurs OpenDNS/Umbrella.

Exemple de modification de la configuration du serveur DNS :

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

Motif

Les machines virtuelles clientes ont été configurées pour utiliser des résolveurs OpenDNS/Umbrella directement au lieu de serveurs DNS publics standard, empêchant ainsi une redirection DNS et une attribution d'identité correctes par le connecteur DNS FTD Umbrella. Lorsque les machines virtuelles pointent explicitement vers des serveurs DNS Umbrella, le pare-feu ne peut pas intercepter, injecter et transférer correctement des requêtes DNS au nom des clients à l'aide de l'organisation et de la stratégie Umbrella configurées.

Prévention et recommandations

- Assurez-vous que les points d'extrémité utilisent des résolveurs DNS standard (DNS interne ou DNS public comme Google DNS) lorsqu'ils se fient au connecteur FTD Umbrella DNS pour l'application.
- Évitez de configurer les clients pour qu'ils pointent directement vers les résolveurs Umbrella/OpenDNS lorsque la redirection ou l'injection DNS est attendue des périphériques de sécurité réseau.
- Validez le flux DNS à l’aide des outils de recherche d’activité Umbrella et de vérificateur de stratégie après toute modification DNS ou de routage.
- Testez le comportement de résolution DNS dans les environnements de production et de travaux pratiques avant le déploiement.

Autres informations utiles

- Configuration du connecteur Umbrella DNS pour Cisco Secure Firewall Management Center
- Renouveler le certificat racine Umbrella pour la configuration basée sur les jetons
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.