Solución de problemas de registro de FTD con Umbrella

Contenido

Problema

El panel de dispositivos de red de Umbrella muestra el Cisco Firewall Management Center (FMC) ya integrado y conectado. El FMC también puede aplicar políticas de Umbrella al FMC e implementarlas en Cisco Firewall Threat Defence (FTD). Sin embargo, el FTD no puede registrarse en Umbrella para redirigir el tráfico DNS.

Entorno

- Cisco Secure Firewall Firepower FTD 10.0.0 (aplicable a las versiones 7.2+)
- Firewall Management Center (FMC) versión 10.0.0 (aplicable a las versiones 7.2+)
- Implementación en entorno de WAN virtual de Azure (aplicable también a modelos de hardware)
- FMC integrado correctamente con Cisco Umbrella
- Configuración del conector Umbrella DNS en FTD

Resolución

Pasos de solución de problemas y análisis

1: Verificar que el FMC esté totalmente integrado y que reciba políticas de Umbrella DNS y que

estén implementadas en el FTD.

- Asegúrese de que el certificado está instalado y es válido.
- Valide que el token de Umbrella y la clave pública estén configurados con resolvers.
- Asegúrese de que se ha aplicado la política general al FTD y de que el estado de registro general indica 200 CORRECTO.

<#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 ABCDEFGHIJKLMNOP12345678900987654321
 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 el estado de registro de Umbrella muestra Unknown, utilice los comandos debugs y show para validar que un grupo de servidores DNS está configurado en las interfaces de datos necesarias para la redirección de Umbrella.

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

Ejemplo de registro de FTD-Umbrella fallido con depuraciones en FTD CLI debido a "No hay interfaces habilitadas" para DNS en la configuración de la plataforma 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 actualización de las configuraciones necesarias para la configuración de la plataforma en el FTD no activa automáticamente el registro de Umbrella de nuevo. Para forzar un nuevo intento de

registro, reinicie el servicio de inspección de DNS en el FTD desde el mensaje 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
```

Ejemplo de registro exitoso de FTD-Umbrella con debugs en 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: Revisar la inspección, inyección y redirección de DNS de FTD a Umbrella mediante depuraciones similares.

<#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
```

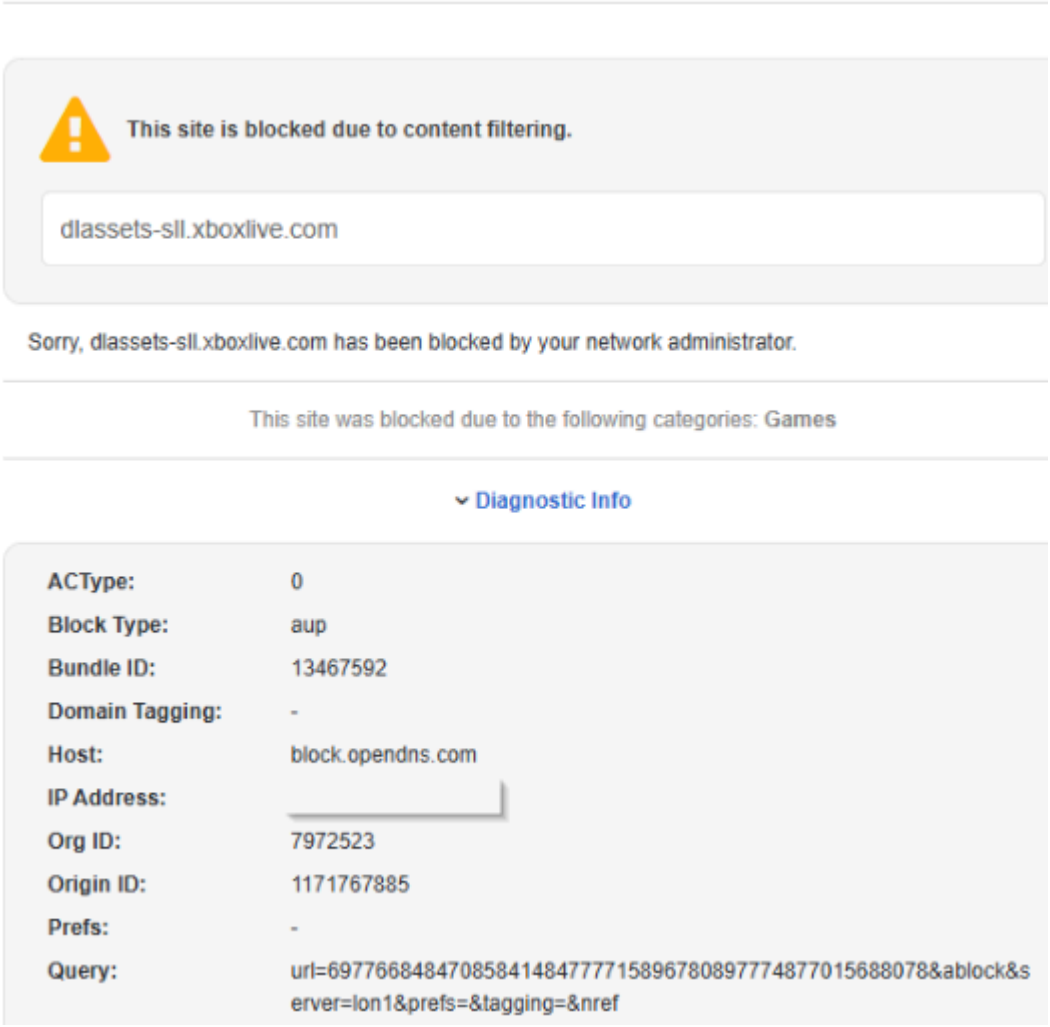
```
Umbrella: modify src: 208.67.220.220 to 208.67.220.220

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: Comprobar los registros de actividad del panel de Umbrella para verificar que el tráfico de FTD llega a Umbrella y que se le están aplicando las políticas de Umbrella. Los usuarios finales ven una página de bloque de Cisco Umbrella que indica la denegación a categorías de sitio específicas, según las configuraciones de políticas.



inline_image_0.png

6: Actualizar la configuración de DNS del usuario final para utilizar servidores DNS públicos en lugar de resolvers OpenDNS/Umbrella directamente.

Ejemplo de cambio de configuración del servidor DNS:

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

Causa

Las máquinas virtuales cliente se configuraron para utilizar resolvers OpenDNS/Umbrella directamente en lugar de servidores DNS públicos estándar, lo que impide la redirección de DNS adecuada y la atribución de identidad por parte del conector DNS Umbrella de FTD. Cuando las VM señalan explícitamente a servidores DNS Umbrella, el firewall no puede interceptar, insertar y reenviar correctamente consultas DNS en nombre de los clientes que utilizan la organización y la política Umbrella configuradas.

Prevención y recomendaciones

- Asegúrese de que los terminales utilizan resoluciones de DNS estándar (DNS interno o DNS público, como DNS de Google) cuando confíe en el conector de DNS de paraguas de FTD para la aplicación.
- Evite configurar los clientes para que apunten directamente a los resolvers de Umbrella/OpenDNS cuando se espere una redirección o inyección de DNS desde los dispositivos de seguridad de la red.
- Valide el flujo de DNS mediante las herramientas de comprobación de políticas y búsqueda de actividad de Umbrella después de cualquier cambio de DNS o de enrutamiento.
- Pruebe el comportamiento de la resolución de DNS en entornos de producción y de laboratorio antes de la implementación.

Contenido relacionado

- Configuración del conector Umbrella DNS para Cisco Secure Firewall Management Center
- Renovación del certificado raíz de Umbrella para la configuración basada en token

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).