Solucionar Problemas de Registro do FTD com o Umbrella

Contents

Problema

O painel Umbrella Network Devices mostra o Cisco Firewall Management Center (FMC) já integrado e conectado. O FMC também pode receber políticas do Umbrella no FMC e implantá-las no Cisco Firewall Threat Defense (FTD). No entanto, o FTD não pode se registrar no Umbrella para redirecionar o tráfego DNS.

Ambiente

- Cisco Secure Firewall Firepower FTD 10.0.0 (aplicável às versões 7.2 e posteriores)
- Firewall Management Center (FMC) versão 10.0.0 (aplicável às versões 7.2 e posteriores)
- Implantação no ambiente de WAN Virtual do Azure (Aplicável também a modelos de hardware)
- FMC integrado com êxito ao Cisco Umbrella
- Configuração do Umbrella DNS Connector no FTD

Resolução

Etapas de Solução de Problemas e Análise

1: Verifique se o FMC está totalmente integrado e recebendo as políticas do Umbrella DNS e se

elas estão implantadas no FTD.

- Verifique se o certificado está instalado e é válido.
- Valide se o token Umbrella e a chave pública estão com os resolvedores configurados.
- Verifique se a política Umbrella foi aplicada ao FTD e se o status de registro Umbrella mostra 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 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: Se o status de registro do Umbrella mostrar Desconhecido, use depurações e comandos show para validar se um grupo de servidor DNS está configurado nas interfaces de dados necessárias para o redirecionamento do Umbrella.

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

Exemplo de falha no registro FTD-Umbrella com depurações no FTD CLI devido a "Nenhuma interface habilitada" para DNS nas Configurações da 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: A atualização das configurações necessárias para as configurações da plataforma no FTD não aciona automaticamente o registro do Umbrella novamente. Para forçar uma nova tentativa de

registro, reinicie o serviço de inspeção DNS no FTD a partir do 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="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
```

Exemplo de registro de FTD-Umbrella bem-sucedido com depurações no 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: Reveja a inspeção, a injeção e o redirecionamento de DNS do FTD para o Umbrella usando depurações semelhantes.

<#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
```

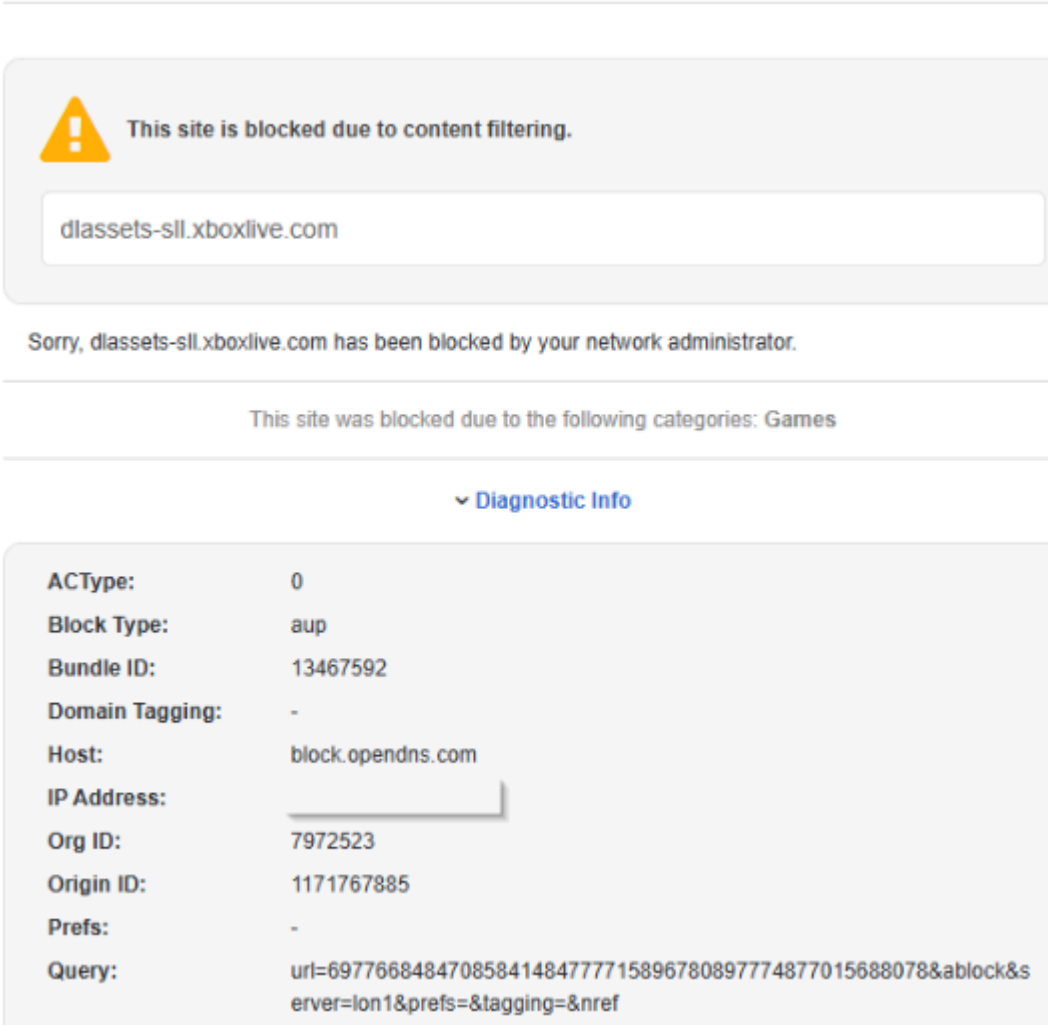
```
Umbrella: modify src: 208.67.220.220 to 208.67.220.220

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: Verifique os logs de Atividade do painel do Umbrella para verificar se o tráfego de FTD atinge o Umbrella e se as políticas do Umbrella estão sendo aplicadas a ele. Os usuários finais veem uma página de bloco do Cisco Umbrella indicando a recusa a categorias de site específicas, com base nas configurações de política.



inline_image_0.png

6: Atualize a configuração DNS do usuário final para usar servidores DNS públicos em vez de resolvedores OpenDNS/Umbrella diretamente.

Exemplo de alteração de configuração de servidor DNS:

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

Causa

As máquinas virtuais do cliente foram configuradas para usar resolvedores OpenDNS/Umbrella diretamente em vez de servidores DNS públicos padrão, impedindo o redirecionamento DNS apropriado e a atribuição de identidade pelo Conector DNS do Umbrella FTD. Quando as VMs apontam explicitamente para servidores DNS do Umbrella, o firewall não pode interceptar, injetar e encaminhar corretamente consultas DNS em nome dos clientes usando a organização e a política do Umbrella configuradas.

Prevenção e recomendações

- Certifique-se de que os pontos de extremidade usem resolvedores DNS padrão (DNS interno ou DNS público, como o Google DNS) ao confiar no FTD Umbrella DNS Connector para aplicação.
- Evite configurar clientes para apontar diretamente para os resolvedores Umbrella/OpenDNS quando for esperado redirecionamento ou injeção de DNS de dispositivos de segurança de rede.
- Valide o fluxo DNS usando as ferramentas de pesquisa de atividade e de verificação de política Umbrella após qualquer alteração de DNS ou roteamento.
- Testar o comportamento da resolução de DNS em ambientes de produção e de laboratório antes da implantação.

Conteúdo relacionado

- Configurando o Umbrella DNS Connector para o Cisco Secure Firewall Management Center
- Renovar Certificado Raiz de Guarda-Chuva para Configuração Baseada em Token

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.