Comprender la función FQDN en Firepower Threat Defence (gestionada por FMC)

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
  - Descripción general de características
  - ¿Qué hay de pre-6.3?
- Configurar
  - Diagrama de la red
  - Arquitectura - Puntos destacados
  - Configuration Steps
- Verificación
- Troubleshoot
  - Recopilar archivos de resolución de problemas de FMC
  - Problemas comunes/mensajes de error
  - Error de implementación
  - Pasos recomendados para la resolución de problemas
  - FQDN no activado
- Preguntas y respuestas

Introducción

Este documento describe la configuración de la función FQDN (a partir de la versión 6.3.0) en Firepower Management Center (FMC) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de administración FirePOWER

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Threat Defense (FTD) Virtual, que ejecuta la versión de software 6.3.0
- Firepower Management Center Virtual (vFMC), que ejecuta la versión de software 6.3.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe la configuración de la función de nombre de dominio completo (FQDN) introducida por la versión 6.3.0 del software en Firepower Management Center (FMC) y Firepower Threat Defence (FTD).

Esta función está presente en el Cisco Adaptive Security Appliance (ASA), pero no en las versiones de software iniciales del FTD.

Asegúrese de que se cumplen estas condiciones antes de configurar los objetos FQDN:

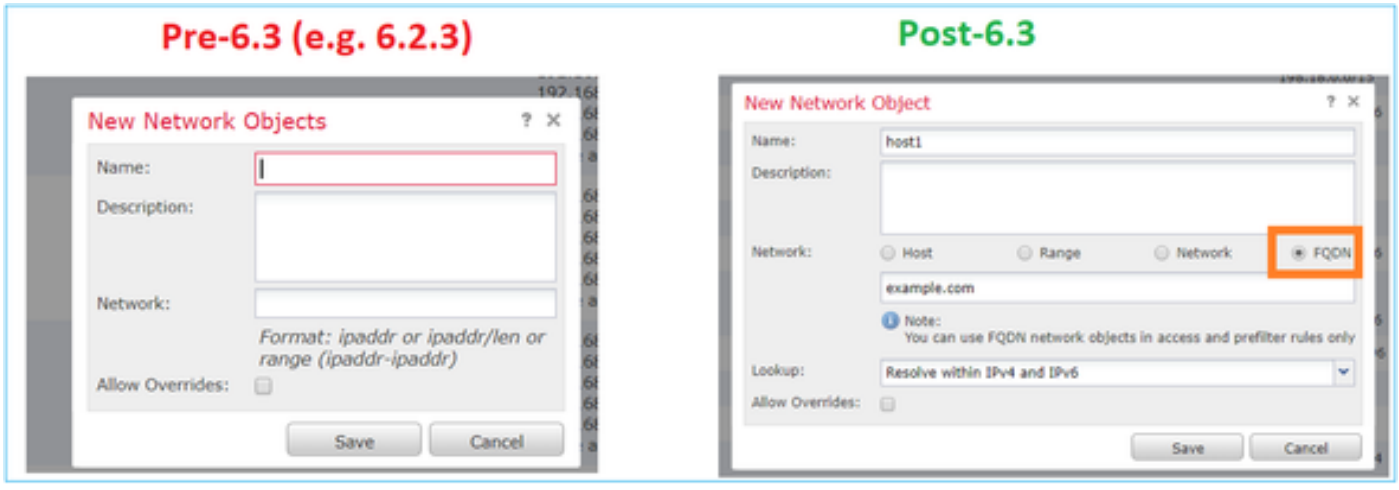
- Firepower Management Center debe ejecutar la versión 6.3.0 o posterior. Puede ser físico o virtual
- Firepower Threat Defence debe ejecutar la versión 6.3.0 o posterior. Puede ser físico o virtual

Descripción general de características

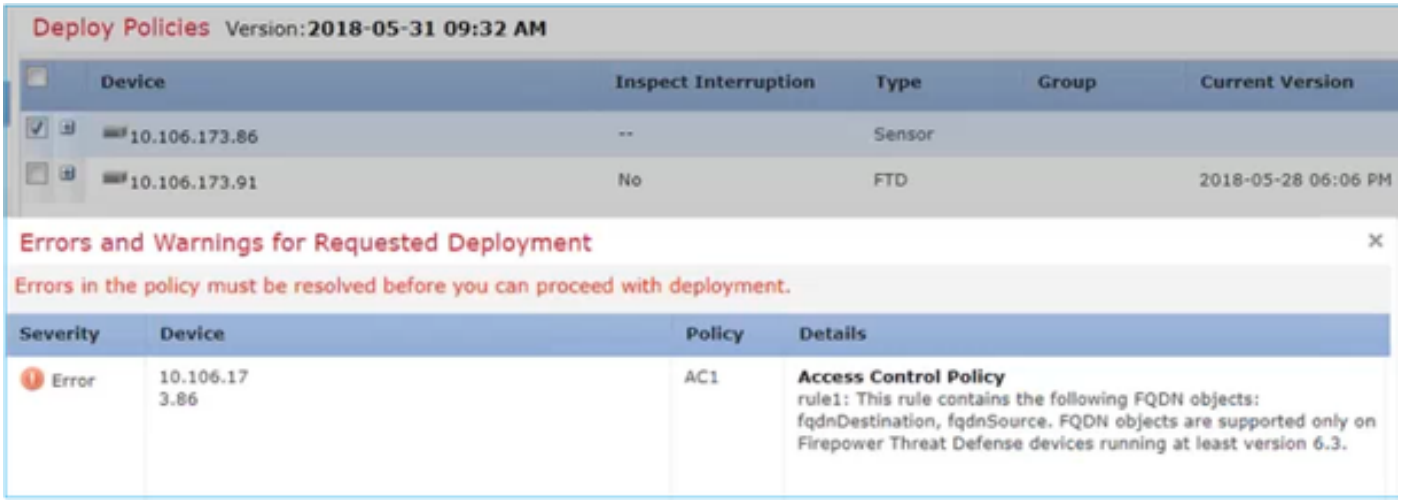
Esta función resuelve un FQDN en una dirección IP y utiliza esta última para filtrar el tráfico cuando una regla de control de acceso o una directiva de filtro previo hacen referencia a ella.

¿Qué hay de pre-6.3?

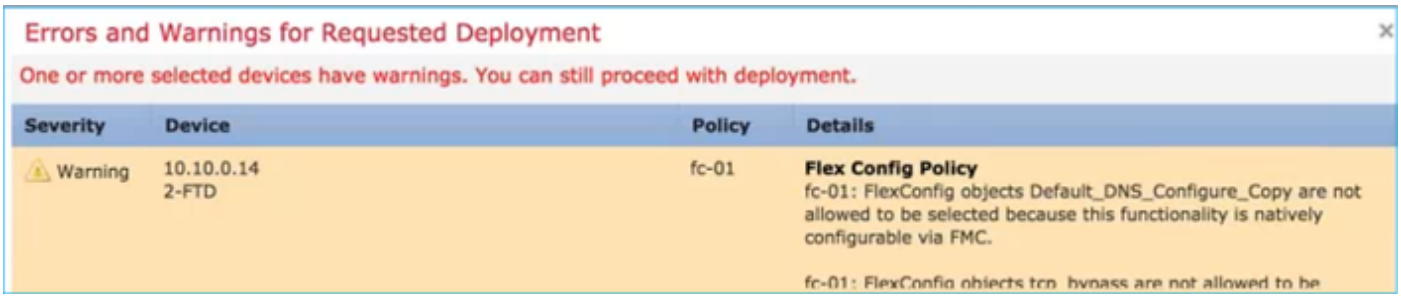
- Los FMC y FTD que ejecutan una versión anterior a la 6.3.0 no pueden configurar objetos FQDN.



- En caso de que FMC ejecute la versión 6.3 o posterior pero FTD ejecute una versión anterior a la 6.3, la implementación de una política muestra este error:

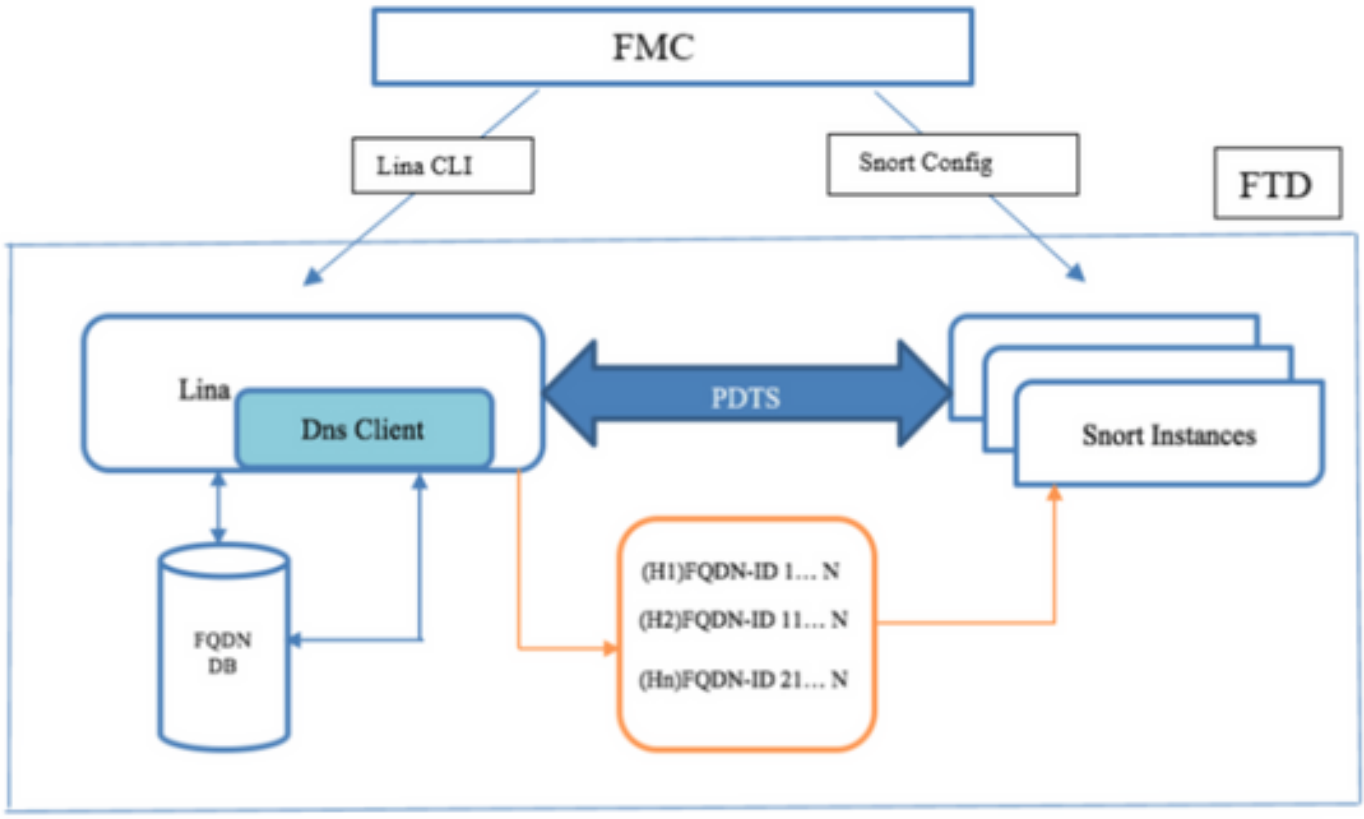


- Además, si configura mediante FlexConfig un objeto DNS, aparece esta advertencia:



Configurar

Diagrama de la red

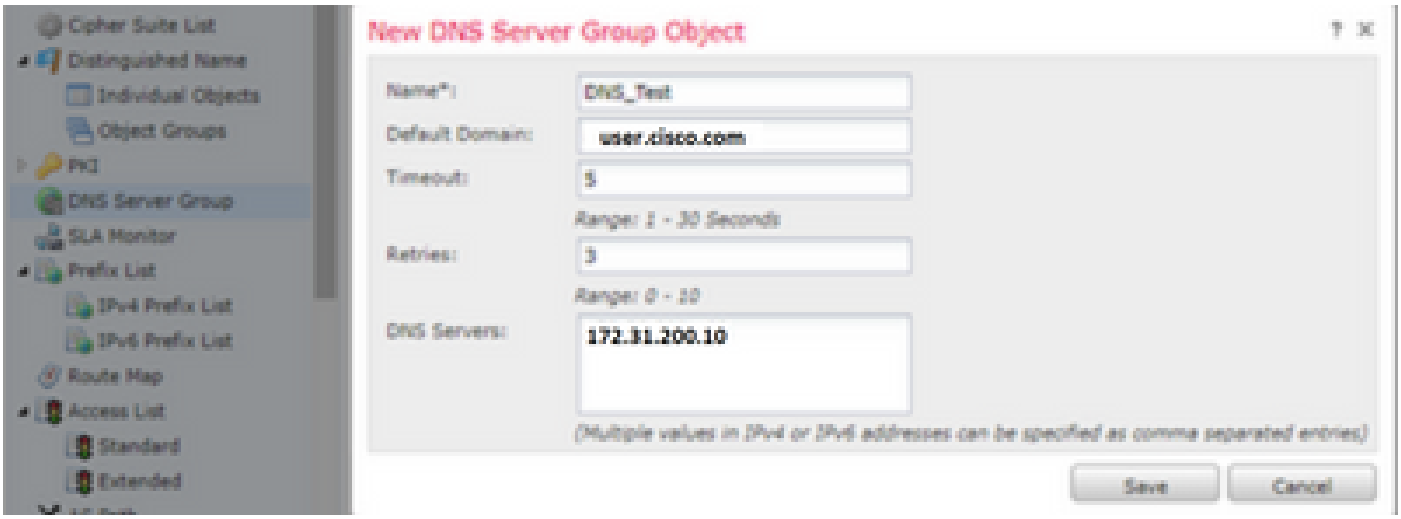


Arquitectura - Puntos destacados

- La resolución de DNS (de DNS a IP) se realiza en LINA
- LINA almacena la asignación en su base de datos
- Por conexión, esta asignación se envía desde LINA a snort
- La resolución del FQDN se produce independientemente de la configuración de alta disponibilidad o de clúster

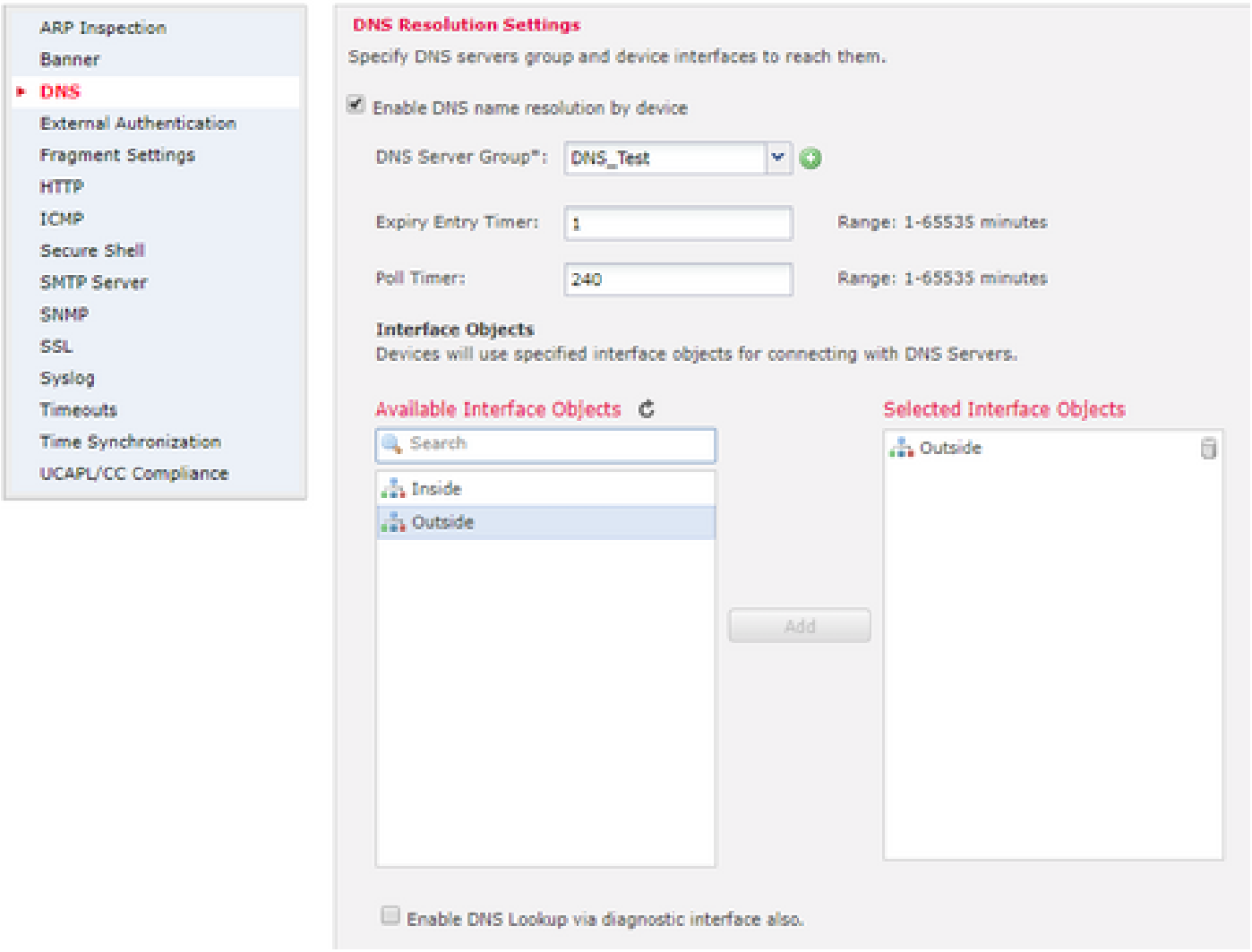
Configuration Steps

Paso 1. Configuración del "objeto de grupo de servidores DNS"



- El nombre del grupo de servidores DNS no debe superar los 63 caracteres
- En una implementación multidominio, los nombres de objeto deben ser únicos en la jerarquía de dominios. El sistema puede identificar un conflicto con el nombre de un objeto que no se puede ver en el dominio actual
- El Dominio Predeterminado (Opcional) se utiliza para anexar a los hostnames que no están completamente calificados
- Los valores predeterminados de los reintentos y del tiempo de espera se rellenan automáticamente.
    - Reintentos: el número de veces, de 0 a 10, que se reintentará la lista de servidores DNS cuando el sistema no reciba una respuesta. El valor predeterminado es 2.
    - Límite de tiempo: el número de segundos, de 1 a 30, antes de que se vuelva a intentar el siguiente servidor DNS. El valor predeterminado es 2 segundos. Cada vez que el sistema reintenta la lista de servidores, este tiempo de espera se duplica.
- Introduzca los servidores DNS que formarán parte de este grupo. Puede ser un formato IPv4 o IPv6 como valores separados por comas
- El grupo de servidores DNS se utiliza para la resolución con el objeto u objetos de interfaz configurados en Configuración de la plataforma
- Se admite la API REST para el objeto CRUD del grupo de servidores DNS

Paso 2. Configurar DNS (configuración de plataforma)



- (Opcional) Modifique los valores de Temporizador de entrada de vencimiento y Temporizador de sondeo en minutos:

La opción de temporizador de entrada de vencimiento especifica el límite de tiempo para quitar la dirección IP de un FQDN resuelto de la tabla de búsqueda de DNS una vez que caduque el tiempo de vida (TTL). Para quitar una entrada es necesario volver a compilar la tabla, por lo que las eliminaciones frecuentes pueden aumentar la carga del proceso en el dispositivo. Este ajuste amplía virtualmente el TTL.

La opción de temporizador de sondeo especifica el límite de tiempo después del cual el dispositivo consulta al servidor DNS para resolver el FQDN que se definió en un grupo de objetos de red. Un FQDN se resuelve periódicamente cuando el temporizador de sondeo ha caducado o cuando el TTL de la entrada IP resuelta ha caducado, lo que ocurra primero.

- (Opcional) Seleccione los objetos de interfaz necesarios de la lista disponible y agréguelos a la lista Objetos de Interfaz Seleccionados y asegúrese de que se puede acceder al servidor DNS a través de las interfaces seleccionadas:

Para los dispositivos Firepower Threat Defence 6.3.0, si no se selecciona ninguna interfaz y la interfaz de diagnóstico está deshabilitada para la búsqueda de DNS, la resolución de DNS se realiza a través de cualquier interfaz que incluya la interfaz de diagnóstico (se aplica el comando

dnsdomain-lookup any).

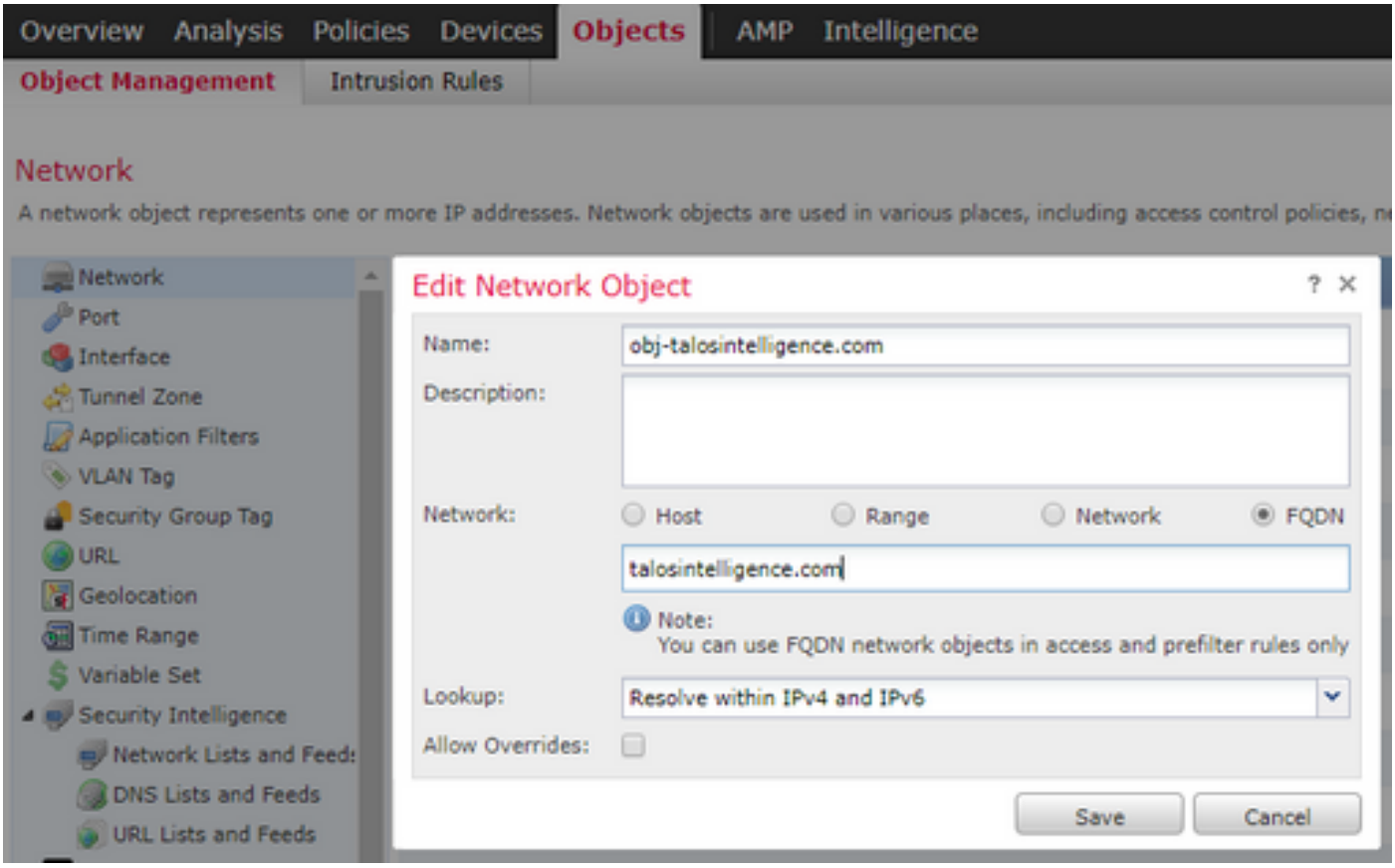
Si no especifica ninguna interfaz y no activa la búsqueda DNS en la interfaz de diagnóstico, el FTD utiliza la tabla de enrutamiento de datos para determinar la interfaz. Si no hay ninguna coincidencia, utiliza la tabla de enrutamiento de administración.

- (Opcional) Seleccione la casilla de verificación Activar búsqueda de DNS también mediante la interfaz de diagnóstico

Si se activa, Firepower Threat Defence utiliza tanto las interfaces de datos seleccionadas como la interfaz de diagnóstico para las resoluciones DNS. Asegúrese de configurar una dirección IP para la interfaz de diagnóstico en la página Dispositivos > Administración de dispositivos > editar dispositivo > Interfaces.

Paso 3. Configuración del FQDN de red de objetos

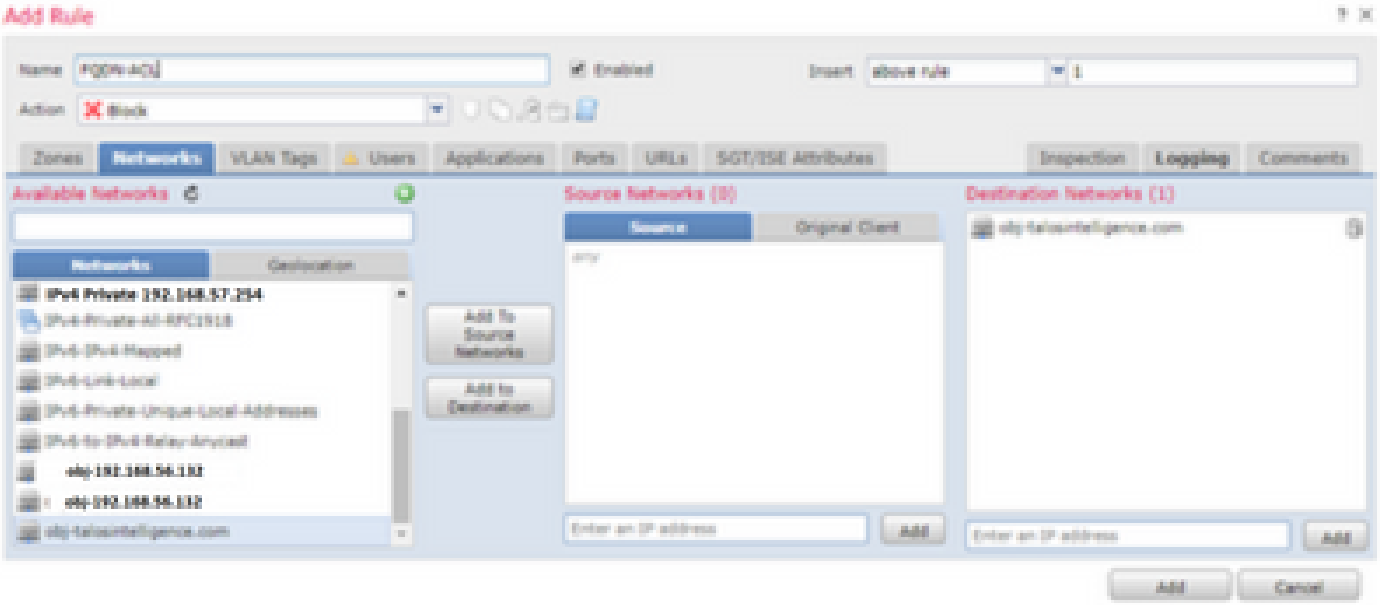
Navegue hasta Objetos > Administración de objetos, dentro de un objeto de red especifique y seleccione la opción FQDN.

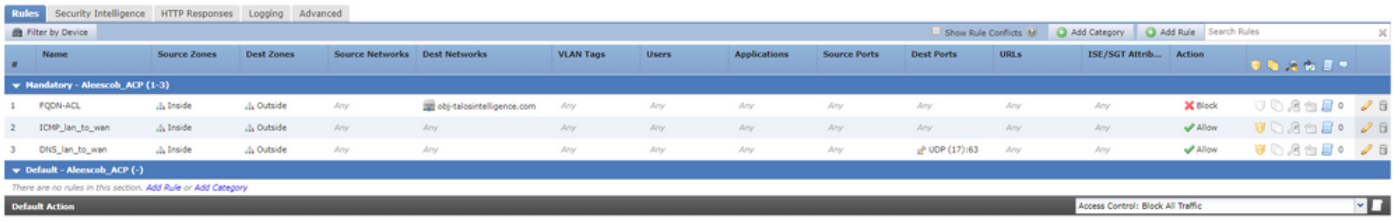


- Se genera un identificador único de 32 bits cuando el usuario crea un objeto FQDN
- Esta ID se transfiere desde FMC a LINA y Snort
- En LINA, esta ID. está asociada al objeto
- En snort, este ID está asociado con la regla de control de acceso que contiene ese objeto

Paso 4. Crear una regla de control de acceso

Cree una regla con el objeto FQDN anterior e implemente la política:





Nota: la primera instancia de la resolución de FQDN se produce cuando el objeto FQDN se implementa en una directiva de control de acceso

Verificación

Utilice esta sección para confirmar que la configuración funciona correctamente.

- Ésta es la configuración inicial de FTD antes de implementar FQDN:

```
aleescob# show run dns
DNS server-group DefaultDNS
```

- Esta es la configuración después de la implementación de FQDN:

```
aleescob# show run dns
dns domain-lookup wan_1557
DNS server-group DNS_Test
```

```
    retries 3
    timeout 5
    name-server 172.31.200.100
    domain-name aleescob.cisco.com
DNS server-group DefaultDNS
dns-group DNS_Test
```

- Así es como se ve el objeto FQDN en LINA:

```
object network obj-talosintelligence.com
 fqdn talosintelligence.com id 268434436
```

- Cuando ya está implementada, el aspecto de la lista de acceso de FQDN es el siguiente en LINA:

```
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
```

- Así es como se ve en Snort (ngfw.rules):

```
# Start of AC rule.
268434437 deny 1 any  any 2 any  any any any  (log dcforward flowstart) (dstfqdn 268434436)
# End rule 268434437
```

Nota: En este escenario, dado que el objeto FQDN se utilizó para el destino, aparece como dstfqdn.

- Si marca los comandos show dns y show fqdn, puede observar que la función ha comenzado a resolver la dirección IP para tallosintelligence:

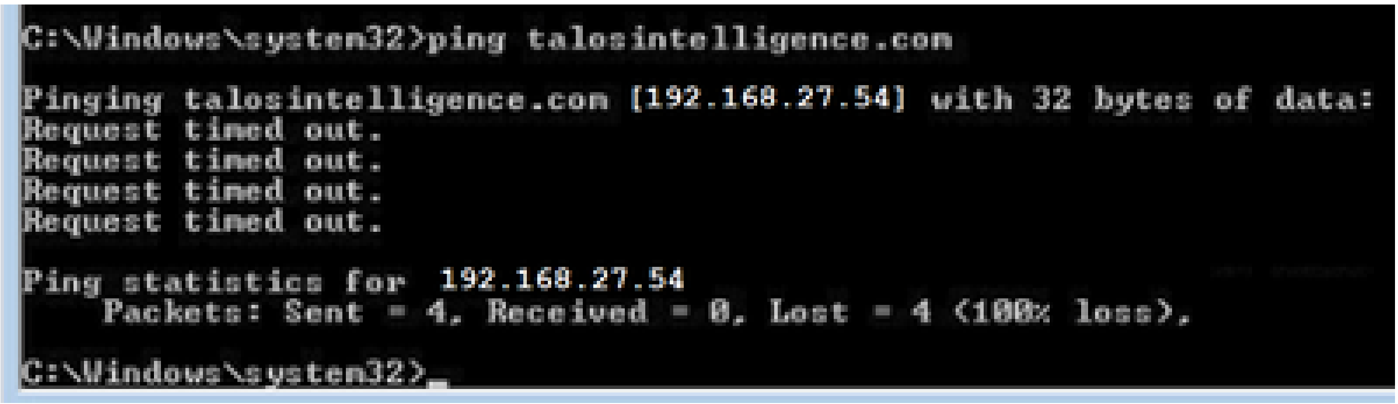
```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36                          TTL 00:05:43
  Address: 2001:DB8::6810:1936                          TTL 00:05:43
  Address: 192.168.27.54                                  TTL 00:05:43
  Address: 192.168.29.54                                  TTL 00:05:43
  Address: 192.168.28.54                                  TTL 00:05:43
  Address: 192.168.26.54                                  TTL 00:05:43
  Address: 192.168.25.54                                  TTL 00:05:43
```

```
aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1c36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1d36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1a36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1936, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.27.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.29.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.28.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.26.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

FQDN ID Detail:
FQDN-ID = 268434436, object = obj-talosintelligence.com, domain = talosintelligence.com
        ip = 2001:DB8::6810:1b36, 2001:DB8::6810:1c36, 2001:DB8::6810:1d36, 2001:DB8::6810:1a36, 2001:DI
```

- Si marca show access-list in LINA, puede observar las entradas expandidas para cada resolución y conteo de aciertos:

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintel
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- Como se muestra en la imagen, un ping a talosintelligence.com falla ya que hay una coincidencia para el FQDN en la lista de acceso. La resolución DNS ha funcionado desde que el FTD bloqueó el paquete ICMP.



- Recuentos de aciertos de LINA para los paquetes ICMP enviados anteriormente:

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelli
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- Las solicitudes ICMP se capturan y se muestran descartadas en la interfaz de ingreso:

aleescob# show cap in 13 packets capture 1: 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp: 192.168.56.132 udp port 59396 unreachable 2: 18:04:12.322126 192.168.56.132 > 1 icmp 72.31.4.161: solicitud de eco 3: 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp: respuesta de eco 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: solicitud de echo 5 18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp: echo reply 6: 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp: echo request 7: 18:04:14.475424 172.31 1.4.161> 192.168.56.132 icmp: echo reply 8: 18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp: echo request 9: 18:04:15.463339 172.31.4.161 > 192.168 56.132 icmp: respuesta de eco 10: 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp: solicitud de eco 11: 18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp: 12: 18:04:35.711480 192.168.56.132 > 192.168.27.54 icmp: echo request 13: 18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp: echo request aleescob# sho cap asp | en 192.168.27.54 162: 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp: echo request 165: 18:04:30.704355 192.168.56.132 > 192.168.2 7.54 icmp: echo request 168: 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp: echo request 176: 18:04:40.707589

192.168.56.132 > 192.168.27.54 icmp:

- Así es como el seguimiento busca uno de estos paquetes ICMP:

```
aleescob# sho cap in packet-number 10 trace

13 packets captured

  10: 18:04:25.713662       192.168.56.132 > 192.168.27.54 icmp: echo request
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.57.254 using egress ifc  wan_1557

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
Additional Information:

Result:
input-interface: lan_v1556
input-status: up
input-line-status: up
output-interface: wan_1557
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

- Si la acción para la regla de control de acceso es Allow (Permitir), este es un ejemplo del

resultado de system support firewall-engine-debug

```
> system support firewall-engine-debug

Please specify an IP protocol: icmp
Please specify a client IP address: 192.168.56.132
Please specify a server IP address:
Monitoring firewall engine debug messages

192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 new firewall session
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 DAQ returned DST FQDN ID: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Starting with minimum 2, 'FQDN-ACL', and SrcZone first wi
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Match found for FQDN id: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 match rule order 2, 'FQDN-ACL', action Allow
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 MidRecovery data sent for rule id: 268434437,rule_action:
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 allow action
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 deleting firewall session
```

- Cuando el FQDN se implementa como parte de un filtro previo (ruta rápida), se muestra de esta manera en ngfw.rules:

```
iab_mode Off
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268434439 fastpath any any  any any any  any any any  (log dcforward both) (tunnel -1)
268434438 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268434438 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268434438 allow any any  any any any  any any 47  (tunnel -1)
268434438 allow any any  any any any  any any 41  (tunnel -1)
268434438 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
```

- Desde el punto de vista de LINA con un paquete rastreado:

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip any object obj-talosintelligence.com rule-id 268434439 event-
access-list CSM_FW_ACL_ remark rule-id 268434439: PREFILTER POLICY: Prefilter-1
access-list CSM_FW_ACL_ remark rule-id 268434439: RULE: FQDN_Prefilter
Additional Information:
```

Troubleshoot

1. Configuración desde FMC

- Compruebe que las directivas y la configuración del servidor DNS están configuradas correctamente
- Comprobar que la implementación se ha realizado correctamente

2. Implementación de comprobación en FTD

- Ejecute show dns y show access-list para ver si se resuelve el FQDN y si se expanden las reglas de AC
- Ejecute show run object network y anote el ID asociado con el objeto (por ejemplo, X para el origen)
- Ejecute show fqdn id X para verificar si el FQDN se resuelve correctamente en la IP de origen
- Verifique si el archivo ngfw.rules tiene una regla AC con el FQDN ID X como origen
- Ejecute system support firewall-engine-debug y verifique el veredicto de Snort

Recopilar archivos de resolución de problemas de FMC

Todos los registros necesarios se recopilan de un FMC Troubleshoot. Para recopilar todos los registros importantes de FMC, ejecute una resolución de problemas desde la GUI de FMC. De lo contrario, desde una indicación de FMC Linux, ejecute sf_Troubleshoot.pl. Si encuentra algún problema, envíe una solución de problemas de FMC con su informe al centro de asistencia técnica Cisco Technical Assistance Center (TAC).

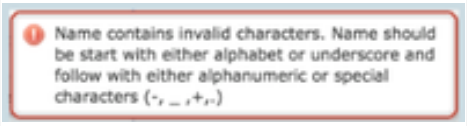
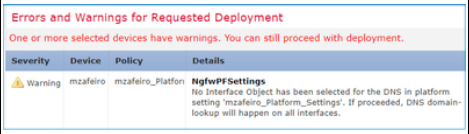
Registros de FMC

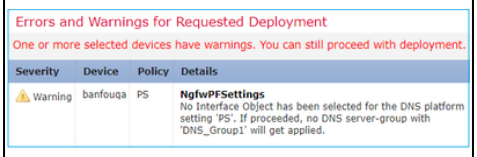
Nombre/ubicación del archivo de registro	Propósito
`/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log`	Todas las llamadas API
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	Todas las llamadas API
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	Registros de generación de CLI
`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Registros de Tomcat

/var/log/mojo.log	Registros de Mojo
/var/log/CSMAgent.log	Llamadas REST entre CSM y DC
/var/log/action_queue.log	Registro de cola de acciones del DC

Problemas comunes/mensajes de error

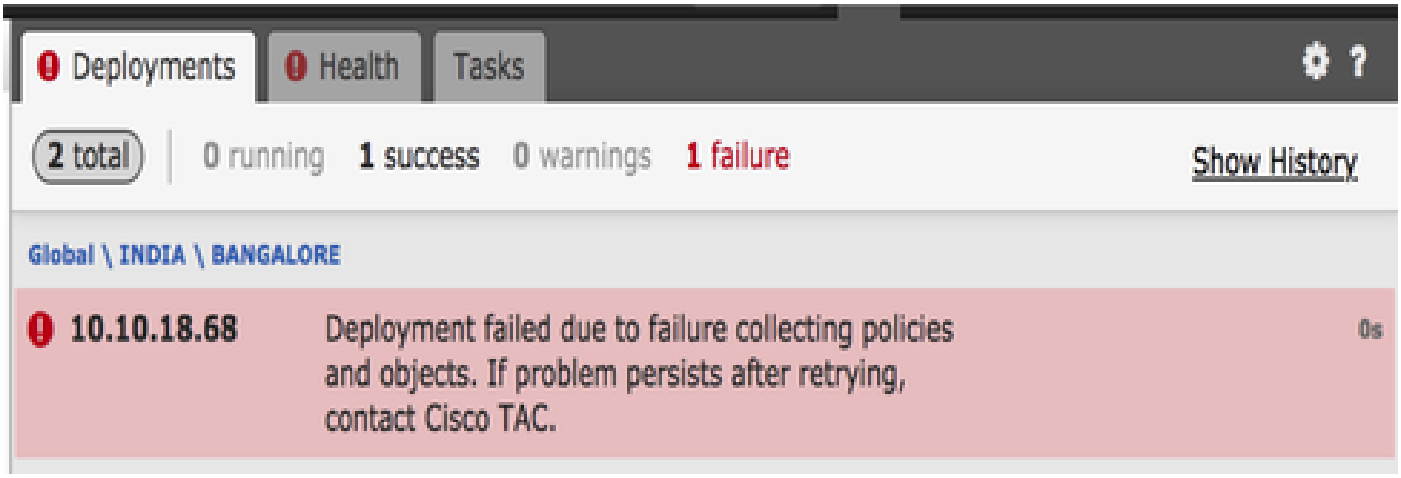
Estos son los errores/advertencias que se muestran en la interfaz de usuario para el objeto de grupo de servidores FQDN y DNS y la configuración de DNS:

Error/advertencia	Situación	Descripción
 El nombre contiene caracteres no válidos. Los nombres deben comenzar con caracteres alfabéticos o de subrayado y, a continuación, alfanuméricos o caracteres especiales. (-,_,+,.)	Usuario configura un nombre incorrecto	Se informa al usuario de la autorización caracteres y rango máximo.
 Valor de dominio predeterminado no válido	El usuario configura un nombre de dominio incorrecto	Se informa al usuario de los caracteres permitidos y del intervalo máximo.
 No se ha seleccionado ningún objeto de interfaz para el DNS en la configuración de plataforma	El usuario no selecciona ninguna interfaz para la búsqueda de dominios Para un dispositivo posterior a la versión 6.3	Se advierte al usuario de que el DNS la CLI del grupo de servidores pronto se aplicará a todas las interfaces.

"mzafeiro_Platform_Settings". Si se procede, la búsqueda de dominio DNS ocurrirá pronto en todas las interfaces		
 No se ha seleccionado ningún objeto de interfaz para el DNS en la configuración de plataforma "mzafeiro_Platform_Settings". Si continúa, no se aplicará pronto ningún grupo de servidores DNS con 'DNS'	El usuario no selecciona ninguna interfaz para la búsqueda de dominios Para un dispositivo 6.2.3	Se advierte al usuario que el DNS la CLI del grupo de servidores no es generado.

Error de implementación

Cuando se utiliza un FQDN en una política que no es una política de AC/política de prefiltro, puede producirse este error y mostrarse en la interfaz de usuario de FMC:



Pasos recomendados para la resolución de problemas

1) Abrir archivo de registro: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Compruebe si hay mensajes de validación similares a:

"Red(s) configurada(s) no válida(s). Redes [RedesQueContienenFQDN] configuradas en los dispositivos[DeviceNames] hacen referencia al FQDN"

3) Acción sugerida:

Verifique si una o más de las políticas mencionadas a continuación ya están configuradas con un FQDN o grupo que contiene uno o varios objetos FQDN y vuelva a intentar la implementación de los mismos después de que se eliminen dichos objetos.

a) Política de identidad

b) Conjuntos de variables que contienen un FQDN aplicado a la política de CA

FQDN no activado

El sistema puede mostrar el siguiente a través de la CLI de FTD:

> show dns INFO: no se ha activado FQDN

El DNS no se activará hasta que se aplique un objeto con un fqdn definido. Una vez aplicado un objeto, se resuelve.

Preguntas y respuestas

P: ¿Es Packet-tracer con FQDN una prueba válida para resolver problemas?
R: Sí, puede utilizar la opción fqdn con packet-tracer.

P: ¿Con qué frecuencia la regla FQDN actualiza la dirección IP del servidor?
R: Depende del valor TTL de la respuesta DNS. Una vez que caduca el valor TTL, el FQDN se resuelve de nuevo con una nueva consulta DNS.
Esto también depende del atributo de temporizador de sondeo definido en la configuración del servidor DNS. La regla FQDN se resuelve periódicamente cuando el temporizador DNS de sondeo ha caducado o cuando el TTL de la entrada IP resuelta ha caducado, lo que ocurra primero.

P: ¿Funciona esto para DNS de ordenamiento cíclico?
R: Los DNS de ordenamiento cíclico funcionan sin problemas, ya que esta función funciona en el FMC/FTD con el uso de un cliente DNS y la configuración de DNS de ordenamiento cíclico se encuentra en el lado del servidor DNS.

P: ¿Hay alguna limitación para los valores de DNS TTL bajos?
R: Si una respuesta DNS incluye 0 TTL, el dispositivo FTD le agrega 60 segundos. En este caso, el valor TTL es de 60 segundos como mínimo.

P.: ¿Por lo tanto, el FTD mantiene el valor predeterminado de 60 segundos?
R: El usuario siempre puede invalidar el TTL con la configuración de Temporizador de entrada de vencimiento en el servidor DNS.

P: ¿Cómo interactúa con las respuestas de DNS de difusión por proximidad? Por ejemplo, los servidores DNS pueden proporcionar diferentes direcciones IP basadas en la geolocalización a los solicitantes. ¿Es posible solicitar todas las direcciones IP para un FQDN? ¿Cómo el comando dig en Unix?
R: Sí, si el FQDN puede resolver varias direcciones IP, todas se enviarán al dispositivo y la regla de CA se expandirá en consecuencia.

P: ¿Hay planes para incluir una opción de vista previa que muestre que los comandos se han enviado antes de que se produzca algún cambio en la implementación?
R: Esto es parte de la opción Preview config disponible a través de Flex config. La vista previa ya está ahí, pero está oculta en la política de Flex Config. Hay un plan para sacarlo y hacerlo genérico.

P: ¿Qué interfaz del FTD se utiliza para realizar la búsqueda de DNS?
R.: Es configurable. Cuando no se configura ninguna interfaz, todas las interfaces con nombre del FTD se habilitan para la búsqueda de DNS.

P: ¿Cada NGFW gestionado realiza su propia resolución DNS y traducción de IP FQDN por separado, incluso cuando se aplica la misma política de acceso a todos ellos con el mismo objeto FQDN?
R.: Sí.

P: ¿Se puede borrar la memoria caché DNS para que las ACL de FQDN resuelvan los problemas?
R: Sí, puede ejecutar los comandos clear dns y clear dns-hosts cache en el dispositivo.

P: ¿Cuándo se activa exactamente la resolución de FQDN?
R: La resolución de FQDN se produce cuando el objeto FQDN se implementa en una política de AC.

P: ¿Es posible purgar la caché solo para un único sitio?
R.: Sí. Si conoce el nombre de dominio o la dirección IP, puede borrarlo, pero no hay un comando como tal según la perspectiva de ACL. Por ejemplo, el comando clear dns host agni.tejas.com está presente para borrar la memoria caché host por host con la palabra clave host como en dns host agni.tejas.com.

P: ¿Es posible utilizar comodines, como *.microsoft.com?
R: No. El FQDN debe comenzar y terminar con un dígito o una letra. Sólo se permiten letras, dígitos y guiones como caracteres internos.

P: ¿La resolución de nombres se realiza en el momento de la compilación de AC y no en el momento de la primera o posteriores solicitudes? Si alcanzamos un TTL bajo (menor que el tiempo de compilación de CA, fast-flux o algo más), ¿se pueden perder algunas direcciones IP?
R: La resolución de nombres se produce tan pronto como se implementa la política de CA. Según la fecha de vencimiento del TTL, se produce la renovación.

P.: ¿Existen planes para procesar la lista de direcciones IP (XML) en la nube de Microsoft Office 365?
R.: No se admite en este momento.

P: ¿El FQDN está disponible en la política SSL?
R: Por ahora no (versión de software 6.3.0). Los objetos FQDN sólo se admiten en la red de origen y de destino para la política de CA únicamente.

P.: ¿Existen registros históricos que puedan proporcionar información sobre los FQDN resueltos? Como los syslogs de LINA, por ejemplo.
R: Para resolver problemas del FQDN en un destino determinado, puede utilizar el comando system support trace. Los seguimientos muestran el ID de FQDN del paquete. Puede comparar el ID para resolver problemas. También puede habilitar los mensajes de Syslog 746015, 746016 para realizar un seguimiento de la actividad de resolución de FQDN dns.

P: ¿Registra el FQDN el dispositivo en la tabla de conexiones con IP resuelta?
R: Para resolver problemas del FQDN en un destino determinado, puede utilizar el comando system support trace, donde los seguimientos muestran el FQDN ID del paquete. Puede comparar el ID para resolver problemas. En el futuro, existen planes para incluir registros de FQDN en el visor de eventos de FMC.

P: ¿Cuáles son las deficiencias de la función de regla FQDN?

R: La función no se amplía si la regla FQDN se utiliza en un destino que cambia la dirección IP con frecuencia (por ejemplo: servidores de Internet que tienen vencimiento TTL de cero), las estaciones de trabajo pueden terminar teniendo nuevas direcciones IP que ya no coinciden con la caché FTD DNS. Como resultado, no coincide con la regla ACP. De forma predeterminada, el FTD agrega 1 minuto además del vencimiento TTL recibido de la respuesta DNS y no se puede establecer en cero. En estas condiciones, se recomienda utilizar la función de filtrado de URL que mejor se adapte a este caso práctico.

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).