Entender o recurso FQDN no Firepower Threat Defense (gerenciado pelo FMC)

Contents

Introdução

Este documento descreve a configuração do recurso FQDN (a partir da v6.3.0) para o Firepower Management Center (FMC) e o Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Threat Defense (FTD) Virtual que executa a versão 6.3.0 do software
- Firepower Management Center Virtual (vFMC) que executa a versão 6.3.0 do software

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve a configuração do recurso Fully Qualified Domain Name (FQDN) introduzido pela versão de software 6.3.0 no Firepower Management Center (FMC) e no Firepower Threat Defense (FTD).

Esse recurso está presente no Cisco Adaptive Security Appliance (ASA), mas não estava nas versões iniciais de software do FTD.

Verifique se estas condições são atendidas antes de configurar objetos FQDN:

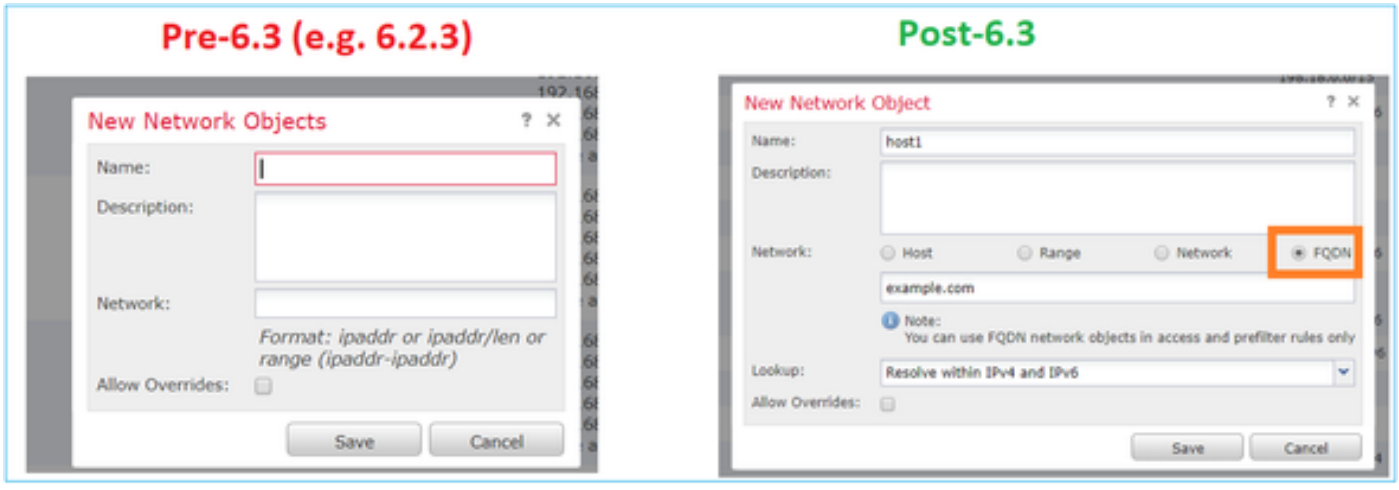
- O Firepower Management Center deve executar a versão 6.3.0 ou posterior. Ele pode ser físico ou virtual
- O Firepower Threat Defense deve executar a versão 6.3.0 ou posterior. Ele pode ser físico ou virtual

Visão geral do recurso

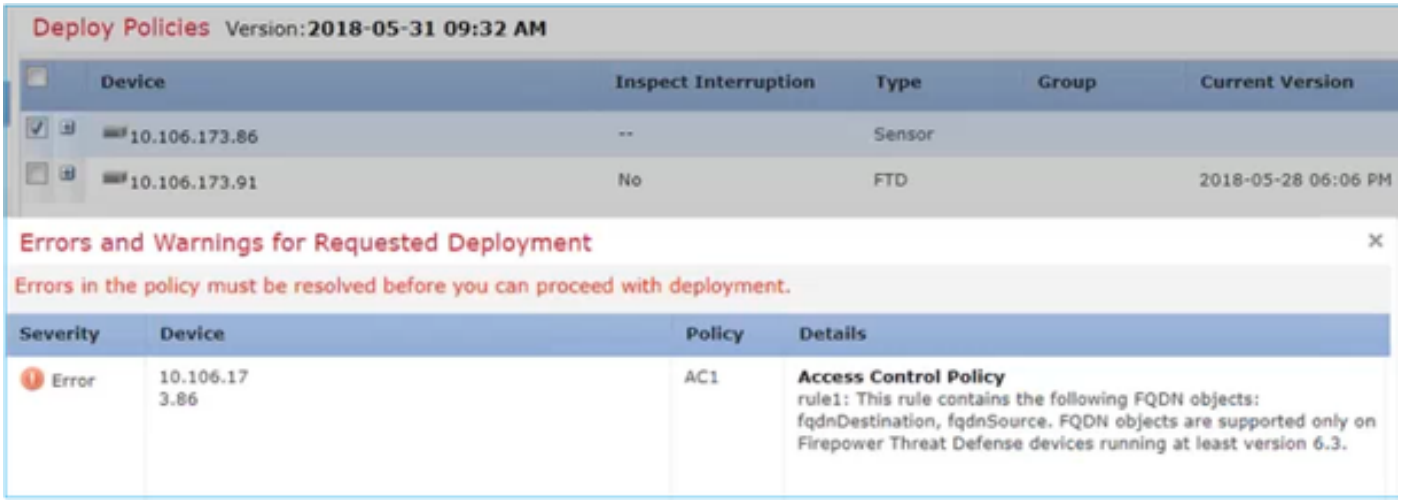
Esse recurso resolve um FQDN em um endereço IP e usa o último para filtrar o tráfego quando referenciado por uma Regra de Controle de Acesso ou Política de Pré-Filtro.

E sobre o pré-6.3?

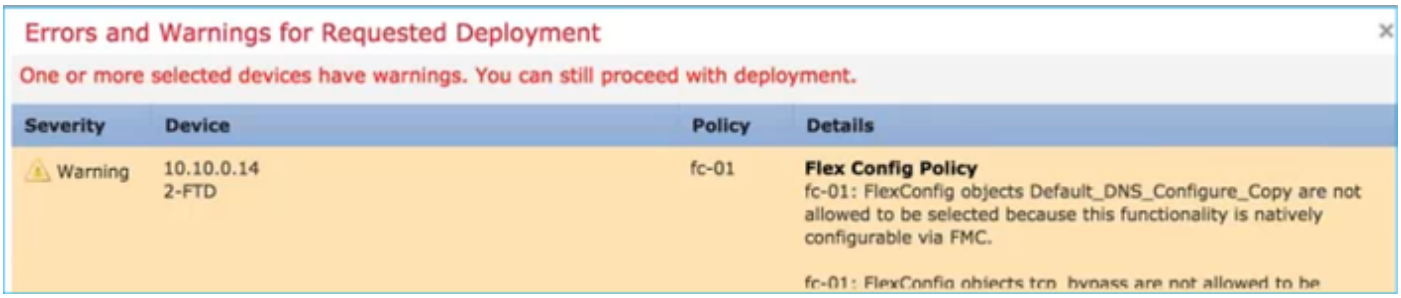
- O FMC e o FTD que executam uma versão anterior à 6.3.0 não podem configurar objetos FQDN.



- Caso o FMC execute a versão 6.3 ou posterior, mas o FTD execute uma versão anterior à 6.3, a implantação de uma política mostra este erro:

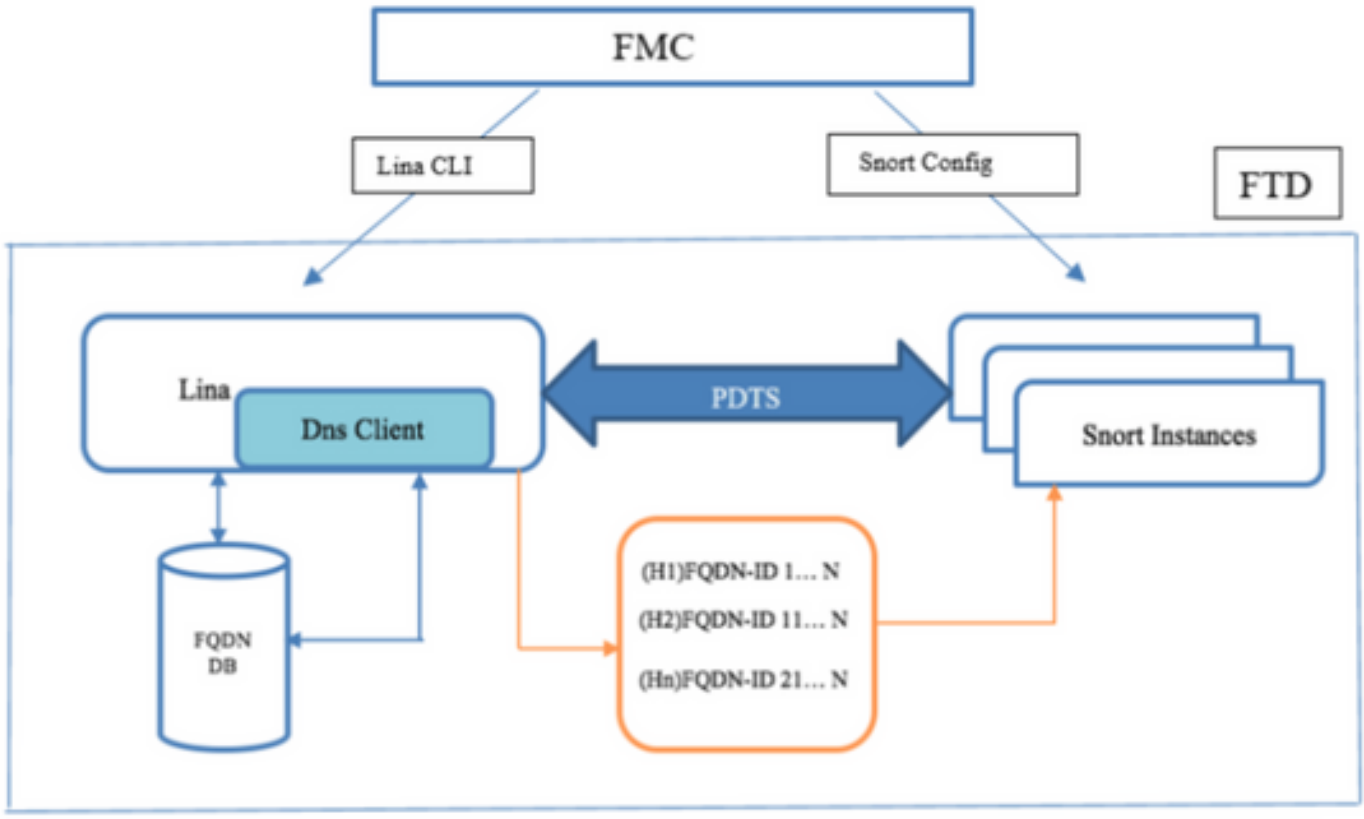


- Além disso, se você configurar via FlexConfig um objeto DNS, este aviso será exibido:



Configurar

Diagrama de Rede

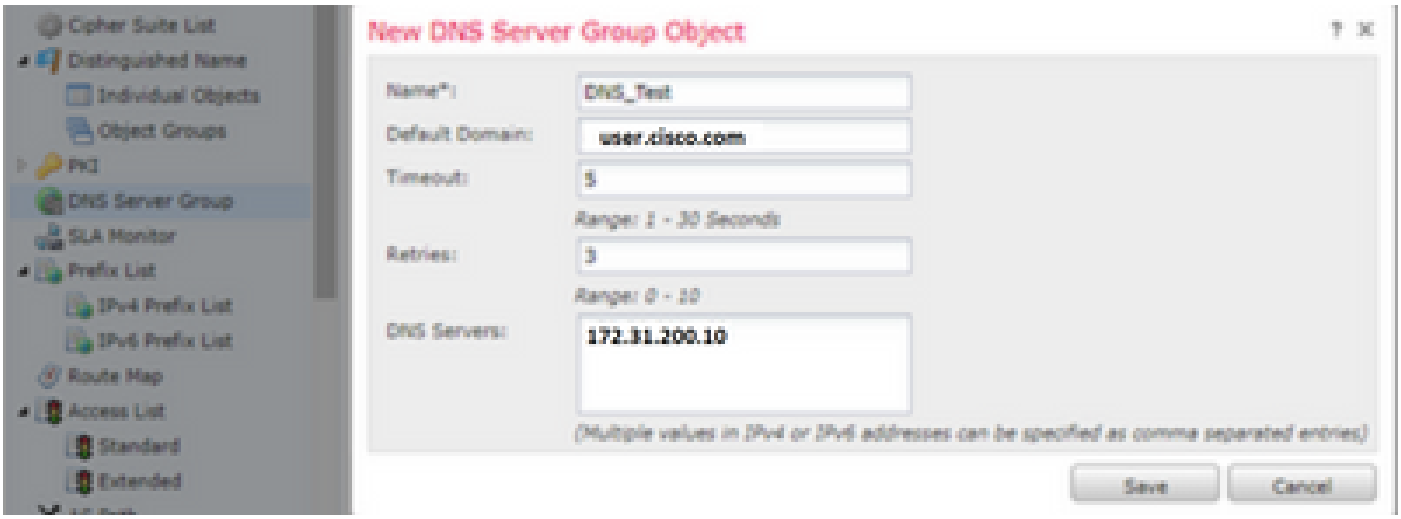


Arquitetura - Pontos principais

- A resolução DNS (DNS para IP) acontece em LINA
- LINA armazena o mapeamento em seu banco de dados
- Em uma base por conexão, esse mapeamento é enviado de LINA para snort
- A resolução do FQDN acontece independentemente da configuração de Alta Disponibilidade ou Cluster

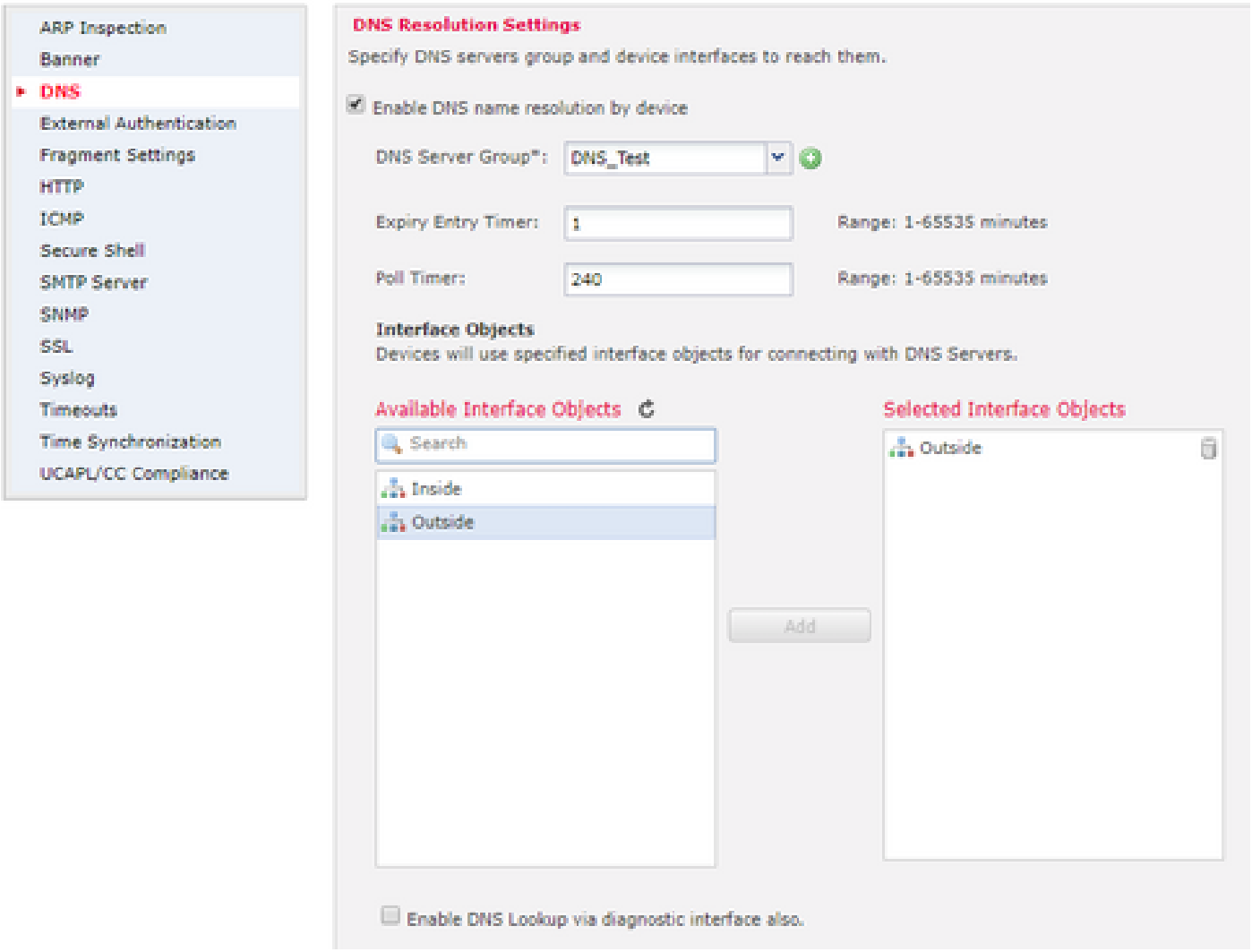
Configuration Steps

Etapa 1. Configurar o "Objeto de Grupo de Servidores DNS"



- O nome do grupo de servidores DNS não deve exceder 63 caracteres
- Em uma implantação de vários domínios, os nomes de objetos devem ser exclusivos dentro da hierarquia de domínio. O sistema pode identificar um conflito com o nome de um objeto que você não pode exibir no domínio atual
- O domínio padrão (opcional) é usado para anexar aos nomes de host que não são totalmente qualificados
- Os valores default de Tentativas e Tempo Limite são pré-preenchidos.
    - Repetições — O número de vezes, de 0 a 10, para repetir a lista de servidores DNS quando o sistema não recebe uma resposta. O padrão é 2.
    - Tempo limite—O número de segundos, de 1 a 30, antes de outra tentativa para o próximo servidor DNS. O padrão é 2 segundos. Cada vez que o sistema repete a lista de servidores, esse tempo limite dobra.
- Insira os servidores DNS que farão parte desse grupo. Pode ser um formato IPv4 ou IPv6 como valores separados por vírgula
- O grupo de servidores DNS é usado para resolução com o objeto ou objetos de interface configurados nas Configurações da plataforma
- Há suporte para a API REST para o objeto CRUD do Grupo de Servidores DNS

Etapa 2. Configurar DNS (Configurações da plataforma)



- (Opcional) Modifique os valores do Cronômetro de entrada de expiração e do Cronômetro de pesquisa em minutos:

A opção de temporizador de entrada de expiração especifica o limite de tempo para remover o endereço IP de um FQDN resolvido da tabela de pesquisa DNS depois que seu Time-to-live (TTL) expirar. Remover uma entrada requer que a tabela seja recompilada, portanto remoções frequentes podem aumentar a carga do processo no dispositivo. Essa configuração estende virtualmente o TTL.

A opção de temporizador de sondagem especifica o limite de tempo após o qual o dispositivo consulta o servidor DNS para resolver o FQDN que foi definido em um grupo de objetos de rede. Um FQDN é resolvido periodicamente quando o temporizador de pesquisa expira ou quando o TTL da entrada IP resolvida expira, o que ocorrer primeiro.

- (Opcional) Selecione os objetos de interface necessários na lista disponível e adicione-os à lista Objetos de interface selecionados e certifique-se de que o servidor DNS esteja acessível através das interfaces selecionadas:

Para dispositivos Firepower Threat Defense 6.3.0, se nenhuma interface for selecionada e a interface de diagnóstico for desabilitada para pesquisa de DNS, a resolução de DNS acontecerá por meio de qualquer interface que inclua a interface de diagnóstico (o comando dnsdomain-

lookup any é aplicado).

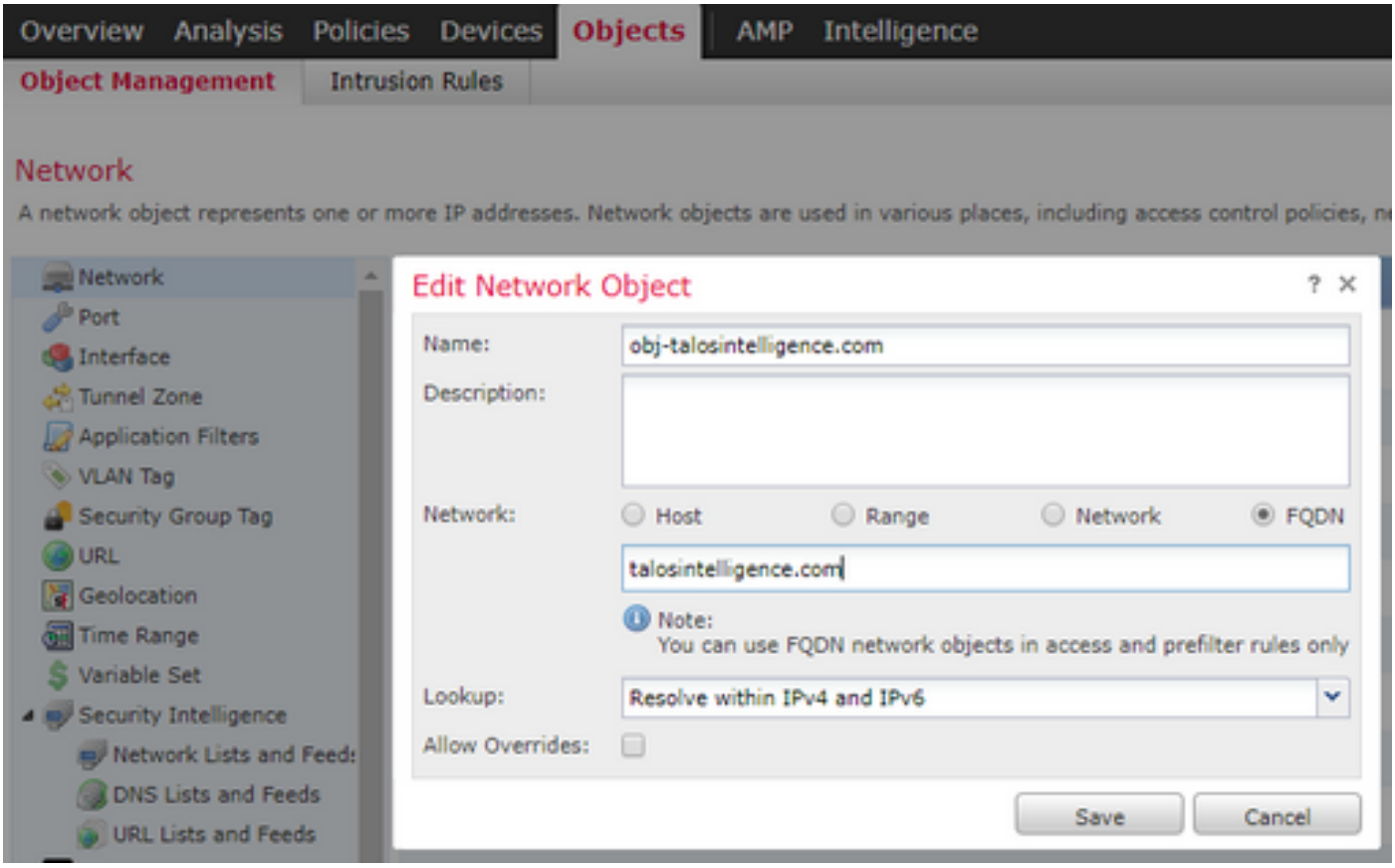
Se você não especificar nenhuma interface—e não ativar a pesquisa DNS na interface de diagnóstico, o FTD usará a Tabela de Roteamento de Dados para determinar a interface. Se não houver correspondência, ele usará a Tabela de Roteamento de Gerenciamento.

- (Opcional) Marque a caixa de seleção Habilitar pesquisa de DNS via interface de diagnóstico também.

Se habilitado, o Firepower Threat Defense usa as interfaces de dados selecionadas e a interface de diagnóstico para resoluções de DNS. Certifique-se de configurar um endereço IP para a interface de diagnóstico na página Dispositivos > Gerenciamento de dispositivo > editar dispositivo > Interfaces.

Etapa 3. Configurar o FQDN da Rede de Objetos

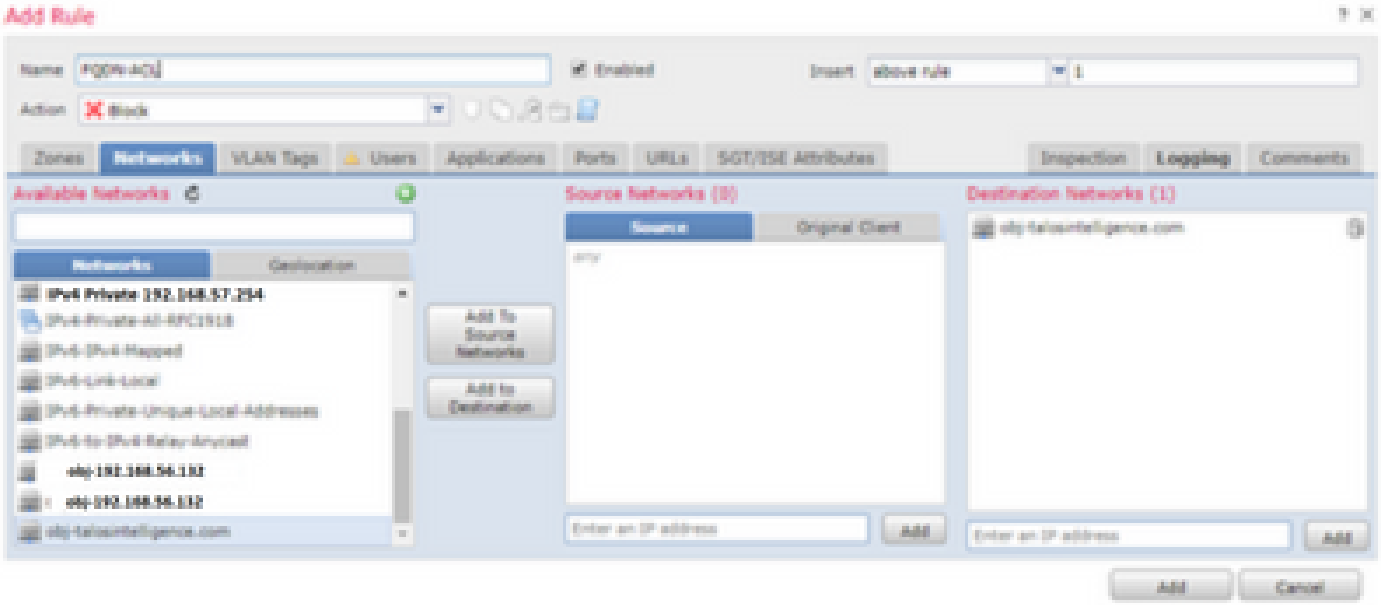
Navegue até Objetos > Gerenciamento de Objetos, em um objeto de rede, especifique e selecione a opção FQDN.

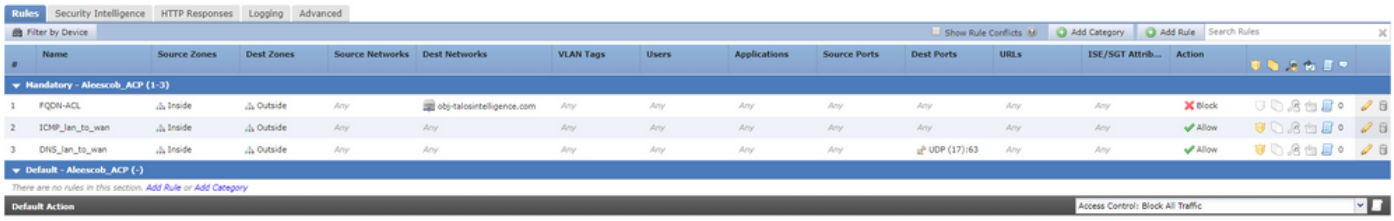


- Uma ID exclusiva de 32 bits é gerada quando o usuário cria um objeto FQDN
- Essa ID é enviada do FMC para LINA e Snort
- No LINA, esse ID é associado ao objeto
- No snort, essa ID é associada à regra de controle de acesso que contém esse objeto

Etapa 4. Criar uma Regra de Controle de Acesso

Crie uma regra com o objeto FQDN anterior e implante a política:





Observação: a primeira instância da resolução FQDN ocorre quando o objeto FQDN é implantado em uma política de controle de acesso

Verificar

Use esta seção para confirmar se sua configuração funciona corretamente.

- Esta é a configuração inicial do FTD antes do FQDN ser implantado:

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

- Esta é a configuração após a implantação do 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
```

- Esta é a aparência do objeto FQDN no LINA:

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

- Quando já está implantada, é assim que a lista de acesso FQDN aparece em 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
```

- Esta é a aparência do 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
```

Observação: neste cenário, como o objeto FQDN foi usado para o destino, ele é listado como dstfqdn.

- Se você marcar os comandos show dns e show fqdn, poderá observar que o recurso começou a resolver o 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
```

- Se você marcar show access-list in LINA, poderá observar as entradas expandidas para cada resolução e contagens de ocorrências:

```
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::6810:1l
  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 mostrado na imagem, um ping para talosintelligence.com falha, pois há uma

correspondência para o FQDN na lista de acesso. A resolução DNS funcionou desde que o pacote ICMP foi bloqueado pelo FTD.

```
C:\Windows\system32>ping talosintelligence.com

Pinging talosintelligence.com [192.168.27.54] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.27.54
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

- Contagens de ocorrências de LINA para os pacotes 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
```

- As solicitações ICMP são capturadas e mostradas descartadas na interface de entrada:

aleescob#show cap em 13 pacotes capturados 1: 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp: 192.168.56.132 porta udp 59396 inalcançável 2: 18:04:12.322126 192.168.56.132 > 172.31.4.161 icmp: echo request 3: 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp: echo reply 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: echo request 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 1 72.31.4.161> 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 > 19 2.168.56.132 icmp: echo reply 10: 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp: echo request 11: 18:04:30.704232 192.168.56.132 > 192.168.2 7.54 icmp: echo request 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 escob#sho cap asp | in 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 icmp 7.54: 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: solicitação de eco

- É assim que o rastreamento procura um destes pacotes 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
```

- Se a ação para a regra de controle de acesso for Permitir, este é um exemplo da saída do comando 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
```

- Quando o FQDN é implantado como parte de um Pré-filtro (Fastpath), é assim que ele fica em 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.
```

- Do ponto de vista LINA com um pacote 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:
```

Troubleshooting

1. Configuração do FMC

- Verifique se as Políticas e as configurações do servidor DNS estão definidas corretamente
- Verificar se a implantação foi bem-sucedida

2. Implantar Verificação no FTD

- Execute show dns e show access-list para ver se o FQDN foi resolvido e as regras de CA foram expandidas
- Execute show run object network e anote a ID associada ao objeto (digamos X para a origem)
- Execute show fqdn id X para verificar se o FQDN foi resolvido corretamente para o IP de origem
- Verifique se o arquivo ngfw.rules tem uma regra AC com FQDN ID X como origem
- Execute o comando system support firewall-engine-debug e verifique o veredito do Snort

Coletar arquivos de solução de problemas do FMC

Todos os registros necessários são coletados de uma solução de problemas do FMC. Para reunir todos os registros importantes do FMC, execute uma Solução de problemas na GUI do FMC. Caso contrário, em um prompt do FMC Linux, execute sf_troubleshoot.pl. Se você encontrar algum problema, envie uma Solução de problemas do FMC com seu relatório para o Centro de assistência técnica da Cisco (TAC).

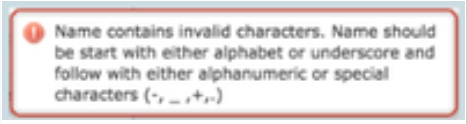
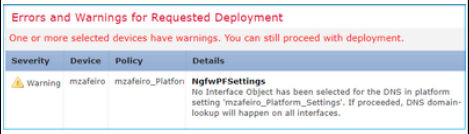
Registros FMC

Nome/local do arquivo de log	Propósito
`/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log`	Todas as Chamadas de API
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	Todas as Chamadas de API
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	Logs de geração de CLI
`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Logs do Tomcat
`/var/log/mojo.log`	Logs Mojo

/var/log/CSMAgent.log	Chamadas REST entre CSM e DC
/var/log/action_queue.log	Log da fila de ações do DC

Problemas comuns/mensagens de erro

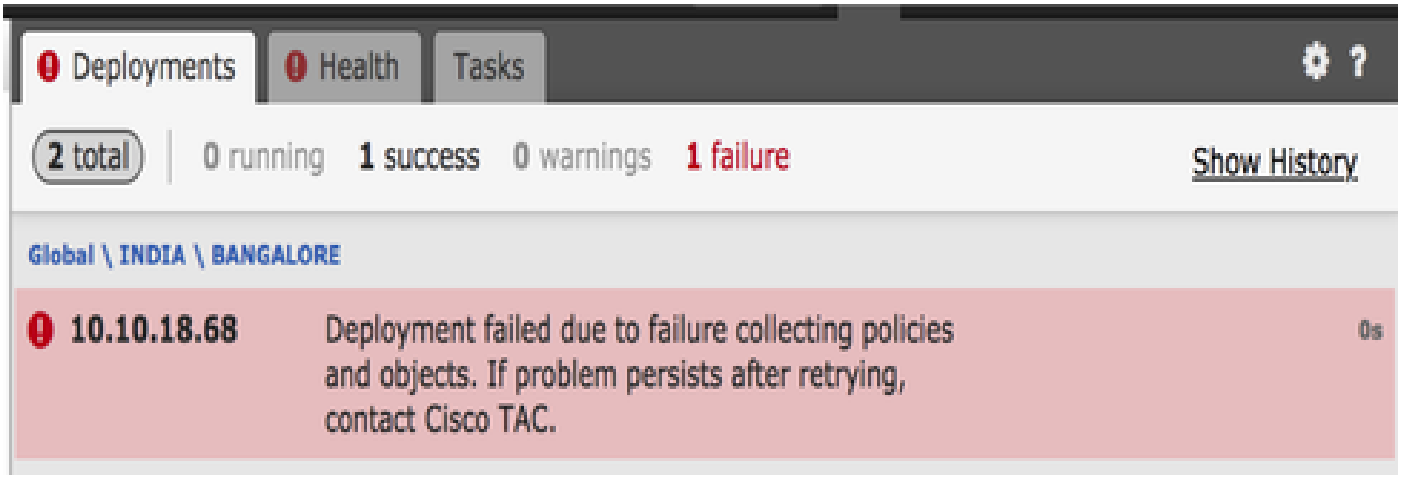
Estes são os erros/avisos mostrados na interface do usuário para o objeto de grupo de servidores FQDN e DNS e Configurações DNS:

Erro/aviso	Cenário	Descrição
 O nome contém caracteres inválidos. Os nomes devem começar com o alfabeto ou o sublinhado e, em seguida, com caracteres alfanuméricos ou especiais. (-,_,+,.)	Usuário configura o nome incorreto	O usuário é informado sobre os caracteres e intervalo máximo.
 Valor de domínio padrão inválido	O usuário configura o nome de domínio incorreto	O usuário é informado sobre os caracteres permitidos e o intervalo máximo.
 Nenhum objeto de interface foi selecionado para o DNS na configuração de plataforma 'mzafeiro_Platform_Settings'. Se continuar, a pesquisa de domínio DNS ocorrerá em breve em todas as interfaces	O usuário não seleciona nenhuma interface para pesquisa de domínio Para um dispositivo pós-6.3	O usuário é avisado de que o DNS a CLI do grupo de servidores será aplicada em breve a todas as interfaces.

 Nenhum objeto de interface foi selecionado para o DNS na configuração de plataforma 'mzafeiro_Platform_Settings'. Se continuar, nenhum grupo de servidores DNS com "DNS" será aplicado em breve	O usuário não seleciona nenhuma interface para pesquisa de domínio Para um dispositivo 6.2.3	O usuário é avisado que o DNS o grupo de servidores CLI não é gerada.

Falha na Implantação

Quando um FQDN é usado em uma política diferente da política de AC/Pré-filtro, esse erro pode ocorrer e ser mostrado na interface do usuário do FMC:



Passos recomendados para solução de problemas

1) Abra o arquivo de registro: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Verifique se há mensagens de validação semelhantes a:

"Redes inválidas configuradas. Redes [NetworksContainingFQDN] configuradas no(s) dispositivo(s) [DeviceNames] referem-se ao FQDN"

3) Ação sugerida:

Verifique se uma ou mais das políticas mencionadas a seguir já estão configuradas com um FQDN ou grupo que contenha objetos FQDN e repita a implantação do mesmo após a remoção desses objetos.

a) Política de identidade

b) Conjuntos de variáveis que contêm um FQDN aplicado à política AC

Nenhum FQDN ativado

O sistema pode mostrar o próximo por meio da CLI do FTD:

> show dns INFO: nenhum FQDN ativado

O DNS não será ativado até que um objeto com um fqdn definido seja aplicado. Depois que um objeto é aplicado, isso é resolvido.

Perguntas e respostas

P: O Packet Tracer com FQDN é um teste válido para solucionar problemas?
R: Sim, você pode usar a opção fqdn com o packet-tracer.

P: Com que frequência a regra FQDN atualiza o endereço IP do servidor?
R: Depende do valor TTL da resposta DNS. Quando o valor TTL expira, o FQDN é resolvido novamente com uma nova consulta DNS.
Isso também depende do atributo do temporizador de pesquisa definido na configuração do servidor DNS. A regra de FQDN é resolvida periodicamente quando o temporizador de DNS da Votação expira ou quando o TTL da entrada de IP resolvida expira, o que ocorrer primeiro.

P: Isso funciona para DNS de rodízio?
R: O DNS de rodízio funciona perfeitamente, pois esse recurso funciona no FMC/FTD com o uso de um cliente DNS e a configuração DNS de rodízio está no lado do servidor DNS.

P: Há uma limitação para os baixos valores TTL DNS?
R: Se uma resposta DNS vem com 0 TTL, o dispositivo FTD adiciona 60 segundos a ele. Nesse caso, o valor do TTL é de no mínimo 60 segundos.

P: Por padrão, o FTD mantém o valor padrão de 60 segundos?
R: O usuário sempre pode substituir o TTL com a configuração Expire Entry Timer no servidor DNS.

P: Como ele interopera com respostas DNS anycast? Por exemplo, os servidores DNS podem

fornecer diferentes endereços IP com base na geolocalização para os solicitantes. É possível solicitar todos os endereços IP para um FQDN? Como o comando dig no Unix?
R: Sim, se o FQDN puder resolver vários endereços IP, todos serão enviados ao dispositivo e a regra AC será expandida de acordo.

P: Há planos para incluir uma opção de visualização que mostre que os comandos são enviados antes de qualquer alteração de implantação?
R: Faz parte da opção Preview config disponível via configuração Flex. A visualização já está lá, mas está oculta na política Flex Config. Há um plano para movê-lo e torná-lo genérico.

P: Qual interface no FTD é usada para executar a pesquisa de DNS?
R: É configurável. Quando nenhuma interface é configurada, todas as interfaces nomeadas no FTD são habilitadas para a pesquisa DNS.

P: Cada NGFW gerenciado executa sua própria resolução de DNS e conversão de IP de FQDN separadamente, mesmo quando a mesma política de acesso é aplicada a todos eles com o mesmo objeto de FQDN?
R: Sim.

P: O cache DNS pode ser limpo para que as ACLs FQDN solucionem problemas?
R: Sim, você pode executar os comandos clear dns e clear dns-hosts cache no dispositivo.

P: Quando exatamente a resolução FQDN é acionada?
R: A resolução FQDN acontece quando o objeto FQDN é implantado em uma política AC.

P: É possível limpar o cache apenas para um único local?
R: Sim. Se você souber o nome do domínio ou o endereço IP, poderá limpá-lo, mas não haverá nenhum comando por perspectiva da ACL. Por exemplo, o comando clear dns host agni.tejas.com está presente para limpar o cache em host por host com a palavra-chave host como em dns host agni.tejas.com.

P: É possível usar curingas, como *.microsoft.com?
R: Não. O FQDN deve começar e terminar com um dígito ou letra. Somente letras, dígitos e hifens são permitidos como caracteres internos.

P: A resolução de nomes é executada no momento da compilação do AC e não no momento da primeira solicitação ou de solicitações subsequentes? Se atingirmos um TTL baixo (menor que o tempo de compilação de AC, fast-flux ou algo do tipo), alguns endereços IP podem ser perdidos?
R: A resolução de nomes acontece assim que a política de CA é implantada. De acordo com a expiração do tempo TTL, a renovação prossegue.

P: Há planos para processar a lista de endereços IP de nuvem (XML) do Microsoft Office 365?
R: Não há suporte para isso no momento.

P: O FQDN está disponível na Política SSL?
R: Não por enquanto (versão de software 6.3.0). Somente há suporte para objetos FQDN nas redes de origem e de destino para a política AC.

P: Há algum log histórico que possa fornecer informações sobre FQDNs resolvidos? Como os syslogs LINA, por exemplo.
R: Para solucionar problemas do FQDN para um destino específico, você pode usar o comando system support trace. Os rastreamentos mostram o ID de FQDN do pacote. Você pode comparar a ID para solucionar o problema. Você também pode habilitar mensagens de Syslog 746015, 746016 para rastrear a atividade de resolução de DNS do FQDN.

P: O dispositivo registra o FQDN na tabela de conexões com o IP resolvido?
R: Para solucionar problemas do FQDN para um destino específico, você pode usar o comando system support trace, onde os rastreamentos mostram o ID do FQDN do pacote. Você pode comparar a ID para solucionar o problema. Há planos para ter registros FQDN no visualizador de eventos no FMC no futuro.

P: Quais são as deficiências do recurso de regra FQDN?

R: O recurso não será escalado se a regra FQDN for usada em um destino que muda o endereço IP com frequência (por exemplo: servidores de Internet que têm TTL expirado como zero), as estações de trabalho podem acabar tendo novos endereços IP que não correspondem mais ao cache DNS do FTD. Como resultado, não corresponde à regra ACP. Por padrão, o FTD adiciona 1 minuto além da expiração do TTL recebido da resposta DNS e não pode ser definido como zero. Nessas condições, é altamente recomendável usar o recurso de filtragem de URL que é mais adequado para esse caso de uso.

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.