Configurar a Alta disponibilidade FTD em dispositivos de FirePOWER

Índice

Introdução

Este documento descreve como configurar e verificar a Alta disponibilidade da defesa da ameaça de FirePOWER (FTD) Failover (ativo/à espera) (HA) em FPR9300.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- corredor da ferramenta de segurança 2xCisco FirePOWER 9300 2.0(1.23)
- FTD que executa 6.0.1.1 (construção 1023)
- Centro de gerenciamento de FirePOWER (FMC) 6.0.1.1 sendo executado (construção 1023)

Tempo da conclusão do laboratório: 1 hora

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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

> **Note**: Em um dispositivo FPR9300 com FTD, você pode configurar somente os inter-chassis HA. As duas unidades em uma configuração HA devem estar conformes as circunstâncias mencionadas aqui.

A tarefa 1. verifica circunstâncias

Exigência da tarefa:

Verifique que ambos os dispositivos FTD cumprem as exigências da nota e ele pode ser configurado como unidades HA.

Solução:

Etapa 1. Conecte ao IP de gerenciamento FPR9300 e verifique o hardware de módulo.

Verifique o hardware FPR9300-1.

```
KSEC-FPR9K-1-A# show server inventory
Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd
Cores
------- ------------ ------------ -------------------- ---------------- ---------------- -------
---
1/1     FPR9K-SM-36  V01          FLM19216KK6          Equipped                   262144
36
1/2     FPR9K-SM-36  V01          FLM19206H71          Equipped                   262144
36
1/3     FPR9K-SM-36  V01          FLM19206H7T          Equipped                   262144
36
KSEC-FPR9K-1-A#
```

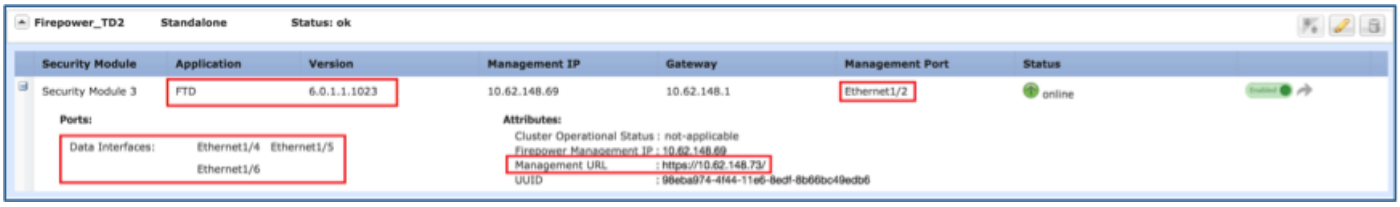
Verifique o hardware FPR9300-2.

```
KSEC-FPR9K-2-A# show server inventory
Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd
Cores
------- ------------ ------------ -------------------- ---------------- ---------------- -------
---
1/1     FPR9K-SM-36  V01          FLM19206H9T          Equipped                   262144
36
1/2     FPR9K-SM-36  V01          FLM19216KAX          Equipped                   262144
36
1/3     FPR9K-SM-36  V01          FLM19267A63          Equipped                   262144
36
KSEC-FPR9K-2-A#
```

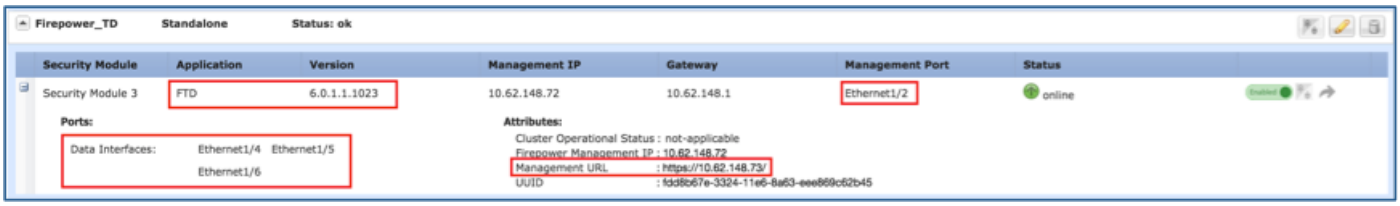
Etapa 2. O log no gerente do chassi FPR9300-1 e navega aos dispositivos lógicos.

Verifique a versão de software, o número e o tipo de relações segundo as indicações das imagens.

FPR9300-1



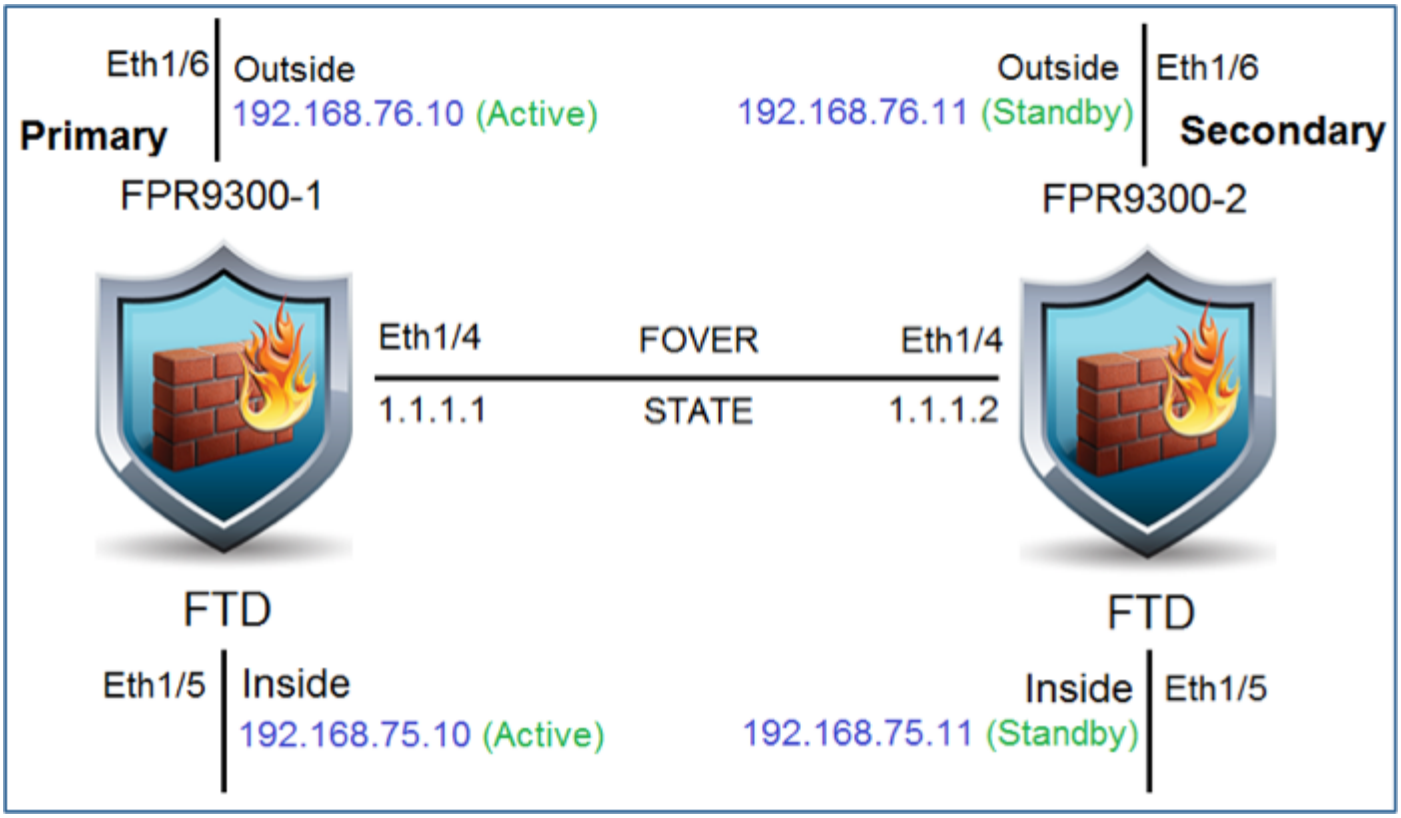
FPR9300-2



A tarefa 2. configura FTD HA em FPR9300

Exigência da tarefa:

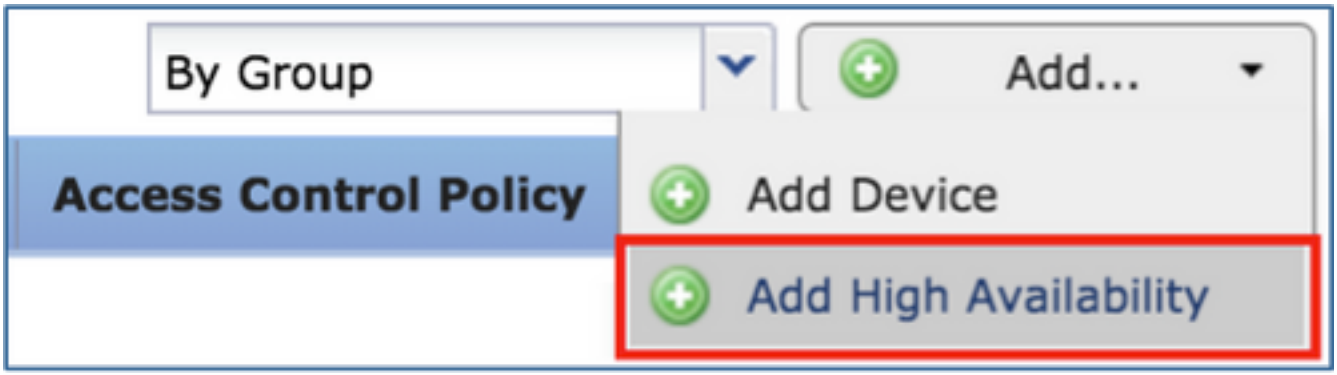
Configurar Failover ativo/à espera (HA) conforme este diagrama.



Solução:

Ambos os dispositivos FTD são registrados já no FMC segundo as indicações da imagem.

Etapa 1. A fim configurar o Failover FTD, para navegar aos **dispositivos > ao Gerenciamento de dispositivos** e a seleto **adicionar a Alta disponibilidade** segundo as indicações da imagem.



Etapa 2. Inscreva o **peer principal** e o **par secundário** e seleto **continua** segundo as indicações da imagem.

Condições

A fim criar um HA entre 2 dispositivos FTD, estas circunstâncias devem ser estadas conformes:

- O mesmo modelo
- A mesma versão (isto se aplica aos FXO e a FTD - (o major (primeiro número), o menor (segundo número), e a manutenção (terceiro número) devem ser iguais))
- O mesmo número de relações
- O mesmo tipo de relações
- Ambos os dispositivos como parte do mesmo grupo/domínio em FMC
- Tenha a configuração idêntica do Network Time Protocol (NTP)
- É distribuído inteiramente no FMC sem as mudanças descomprometidos
- Reaja do mesmo modo de firewall: roteado ou transparente.
- Note que isto deve ser verificado nos dispositivos FTD e no FMC GUI desde que houve os casos onde o FTDs teve o mesmo modo, mas FMC não reflete este.
- Tenha o Point-to-Point Protocol sobre Ethernet (PPPoE) DHCP configurado em algumas das relações
- Hostname diferente (nome de domínio totalmente qualificado (FQDN)) para ambos os chassis. A fim verificar o hostname do chassi vá a FTD CLI e execute este comando:

```
firepower# show chassis-management-url

https://KSEC-FPR9K-1.cisco.com:443//
```

Se ambos os chassis têm o mesmo nome, mude o nome em um deles com o uso destes comandos:

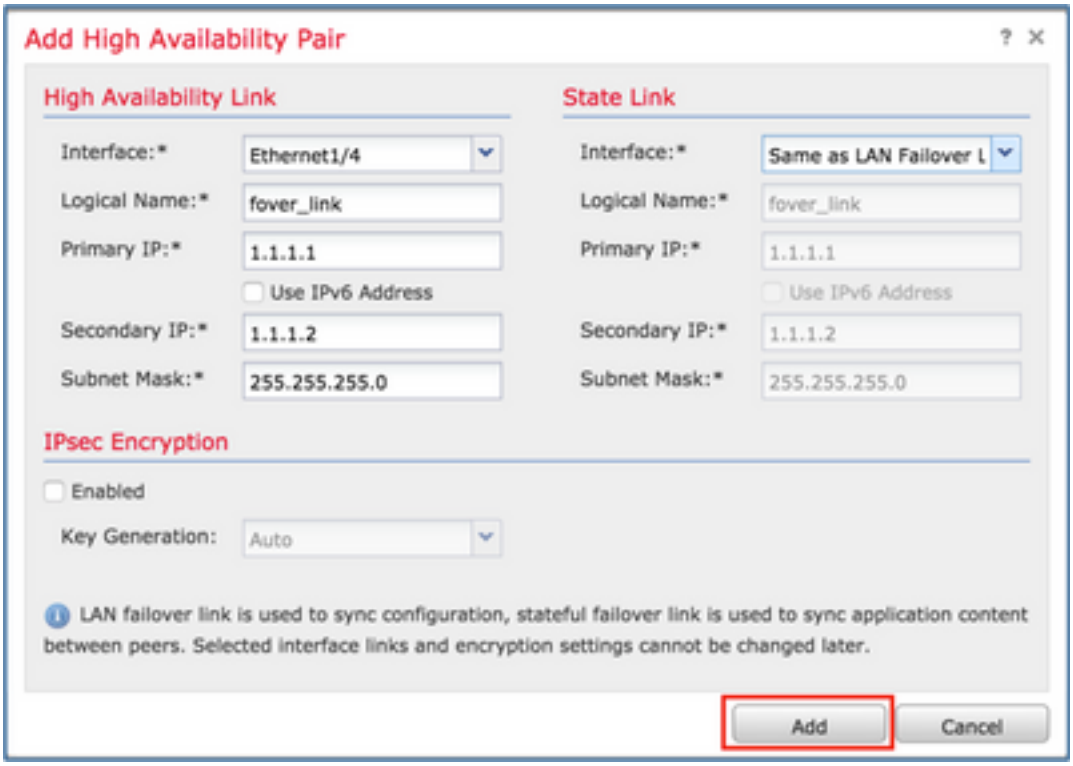
```
KSEC-FPR9K-1-A# scope system
KSEC-FPR9K-1-A /system # set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* # commit-buffer
FPR9K-1-A /system # exit
FPR9K-1new-A#
```

Depois que você muda os chassis nomeiam, removem registro o FTD do FMC e registrar-lo outra vez. Então, continue com a criação de pares HA.

Etapa 3. Configurar o HA e indique os ajustes dos links.

Em seu caso, o link do estado tem os mesmos ajustes que a Alta disponibilidade do link.

Seleto **adicionar** e espere por alguns minutos pelos pares HA a ser distribuídos segundo as indicações da imagem.

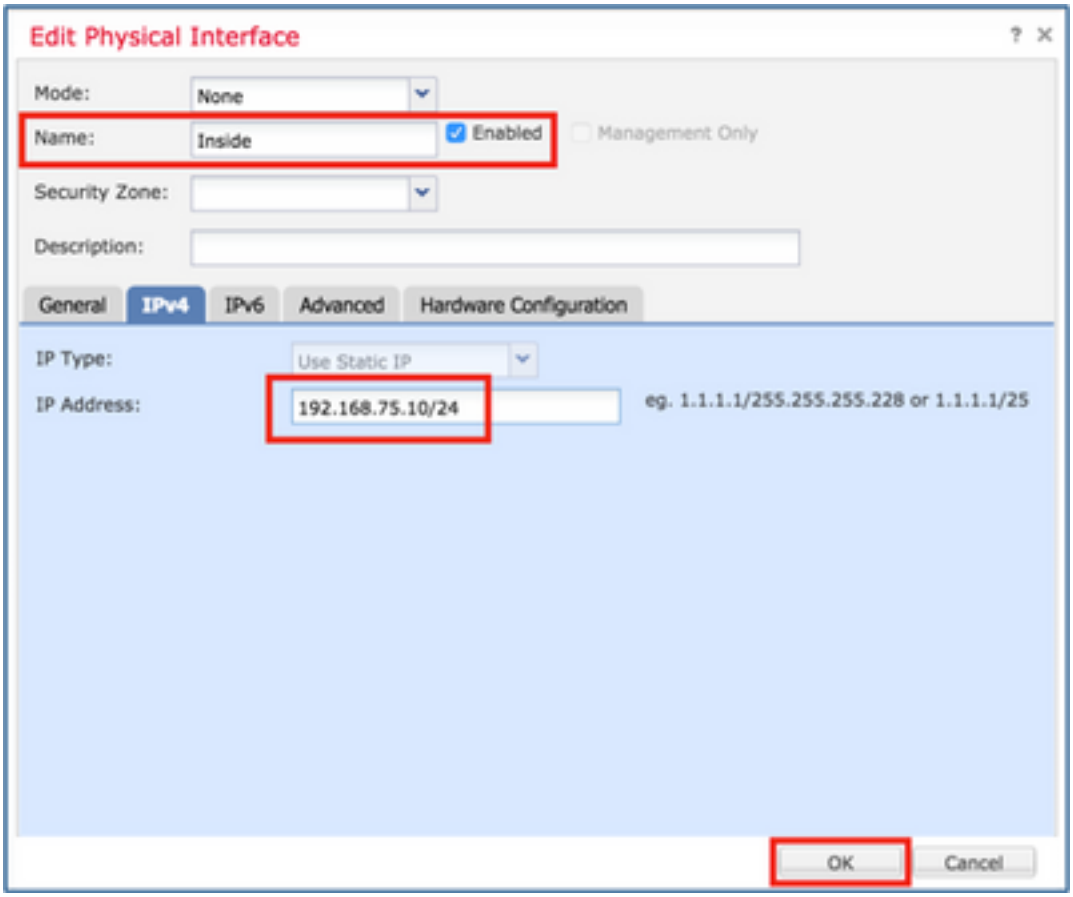


Etapa 4. Configurar as interfaces de dados (preliminares e os endereços IP em standby)

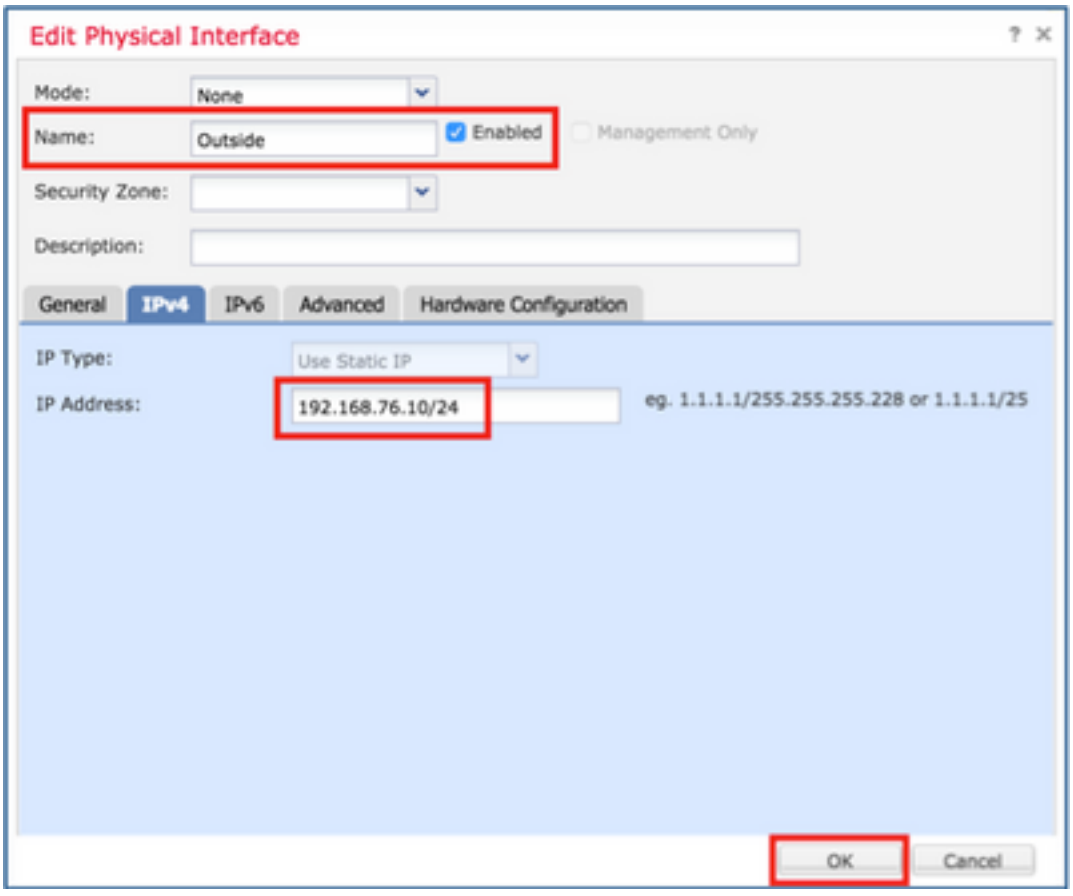
Do FMC GUI, clique sobre o HA **editam** segundo as indicações da imagem.

Etapa 5. Configurar os ajustes da relação segundo as indicações das imagens.

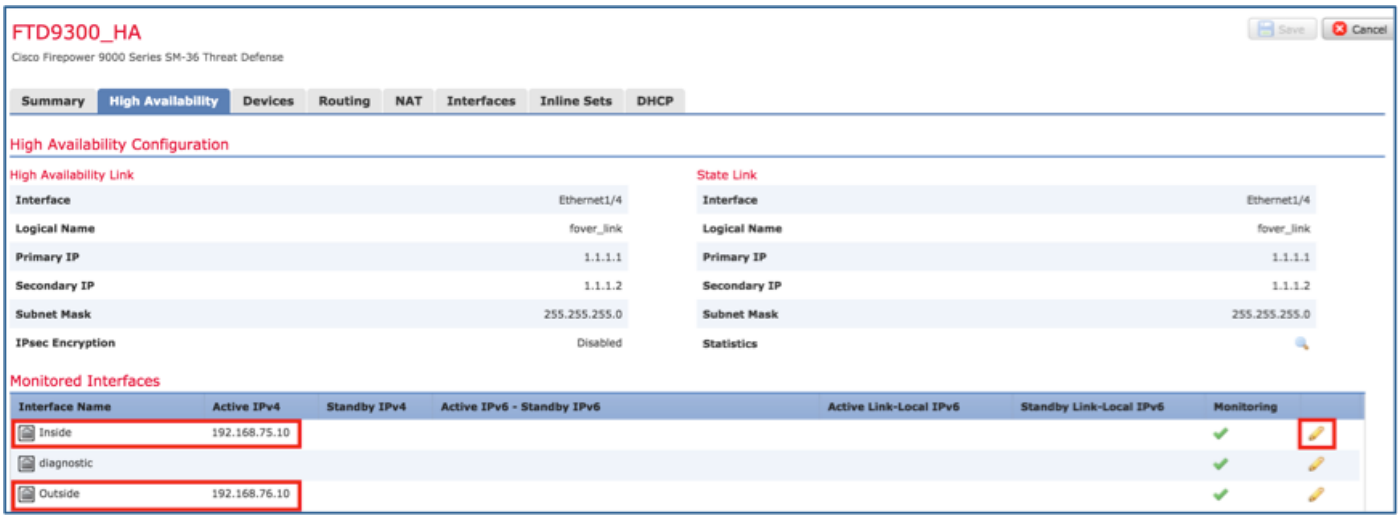
Ethernet 1/5 de relação.



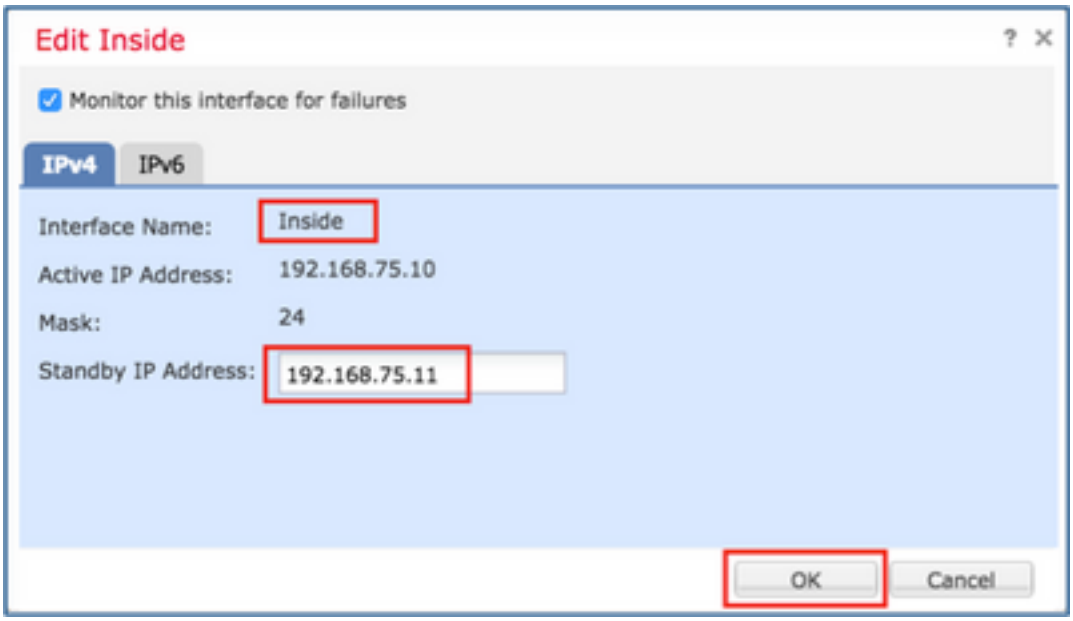
Ethernet 1/6 de relação.



Etapa 6. Navegue à **Alta disponibilidade** e clique sobre o nome da relação **editam** para adicionar os endereços IP em standby segundo as indicações da imagem.

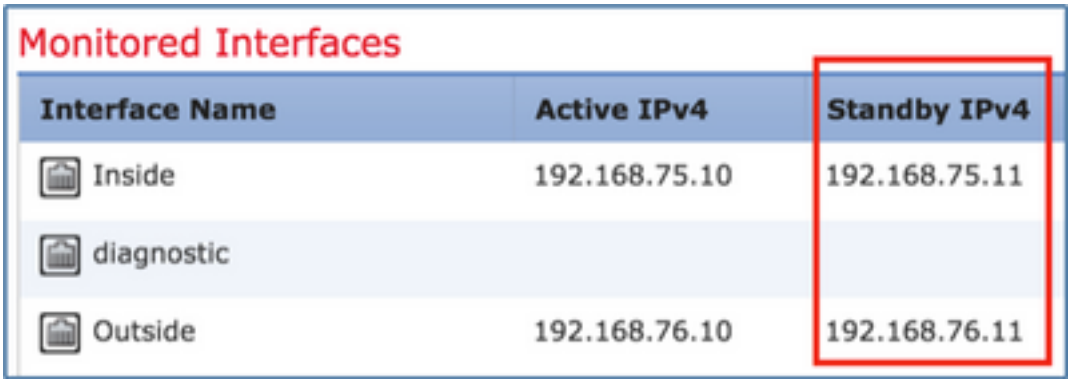


Etapa 7. Para a interface interna segundo as indicações da imagem.

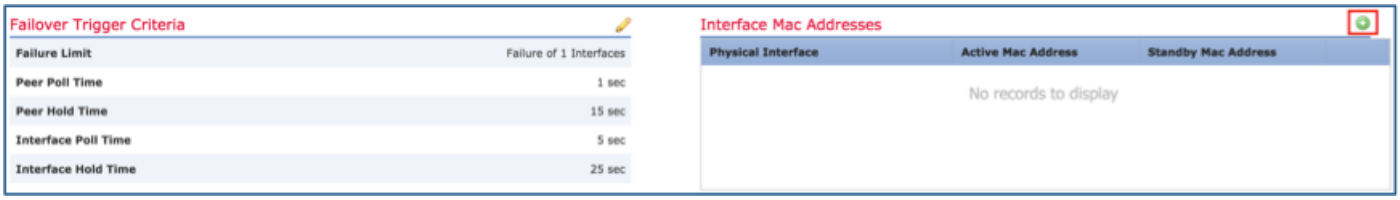


Etapa 8. Faça o mesmos para a interface externa.

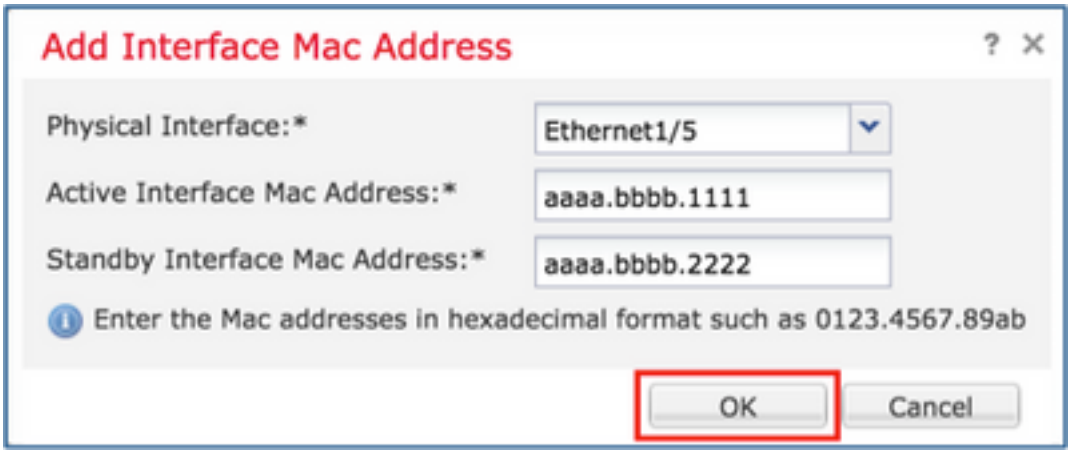
Etapa 9. Verifique o resultado segundo as indicações da imagem.



Etapa 10. Ficar na Alta disponibilidade da aba e configurar endereços MAC virtuais segundo as indicações da imagem.



Etapa 11. Para a interface interna é segundo as indicações da imagem.



Etapa 12. Faça o mesmos para a interface externa.

Etapa 13. Verifique o resultado segundo as indicações da imagem.

Etapa 14. Depois que você configura as mudanças, selecione a **salvaguarda** e distribua-a.

A tarefa 3. verifica FTD HA e licenciar

Exigência da tarefa:

Verifique os ajustes FTD HA e as licenças permitidas do FMC GUI e de FTD CLI.

Solução:

Etapa 1. Navegue ao **sumário** e verifique os ajustes HA e as licenças permitidas segundo as indicações da imagem.

Etapa 2. Do FTD CLISH CLI, execute estes comandos:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours FLM19267A63, Mate FLM19206H7T
Last Failover at: 18:32:38 EEST Jul 21 2016
This host: Primary - Active
Active time: 3505 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0)  status (up)
slot 2: diskstatus rev (1.0)  status (up)
Other host: Secondary - Standby Ready
Active time: 172 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0)  status (up)
slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
Link : fover_link Ethernet1/4 (up)
Stateful Obj xmit       xerr       rcv        rerr
General417        0          416        0
sys cmd  416        0          416        0
up time  0          0          0          0
RPC services  0          0          0          0
TCP conn 0          0          0          0
UDP conn 0          0          0          0
ARP tbl  0          0          0          0
Xlate_Timeout  0          0          0          0
IPv6 ND tbl  0          0          0          0
VPN IKEv1 SA 0          0          0          0
VPN IKEv1 P2 0          0          0          0
VPN IKEv2 SA 0          0          0          0
VPN IKEv2 P2 0          0          0          0
VPN CTCP upd 0          0          0          0
VPN SDI upd 0          0          0          0
VPN DHCP upd 0          0          0          0
SIP Session 0          0          0          0
SIP Tx 0          0          0          0
```

```
SIP Pinhole 0          0          0          0
Route Session 0          0          0          0
Router ID 0          0          0          0
User-Identity 1          0          0          0
CTS SGTNAME 0          0          0          0
CTS PAC 0          0          0          0
TrustSec-SXP 0          0          0          0
IPv6 Route 0          0          0          0
STS Table 0          0          0          0

Logical Update Queue Information
  Cur Max Total
Recv Q: 0 10 416
Xmit Q: 0 11 2118

>
```

Etapa 3. Faça o mesmos no dispositivo secundário.

Etapa 4. Execute o comando do **estado do Failover da mostra da** LINA CLI:

```
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             18:32:56 EEST Jul 21 2016

====Configuration State===
Sync Done
====Communication State===
Mac set

firepower#
```

Etapa 5. Verifique a configuração running da unidade primária (LINA CLI):

```
firepower# show running-config failover
failover
failover lan unit primary
failover lan interface fover_link Ethernet1/4
failover replication http
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link fover_link Ethernet1/4
failover interface ip fover_link 1.1.1.1 255.255.255.0 standby 1.1.1.2
firepower#

firepower# show running-config interface
!
interface Ethernet1/2
 management-only
 nameif diagnostic
 security-level 0
 no ip address
!
interface Ethernet1/4
 description LAN/STATE Failover Interface
!
interface Ethernet1/5
 nameif Inside
```

```
 security-level 0
 ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
interface Ethernet1/6
 nameif Outside
 security-level 0
 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
firepower#
```

Encarregue 4. papéis de comutação do Failover

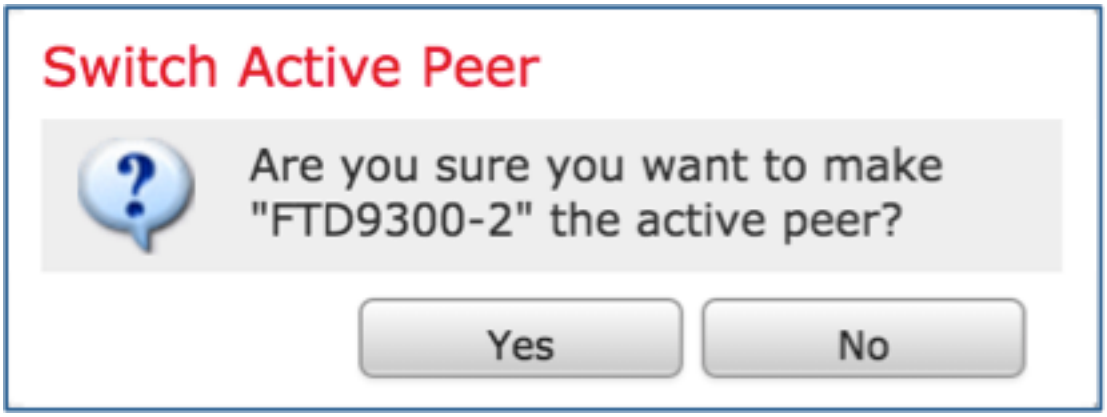
Exigência da tarefa:

Do FMC, comute os papéis do Failover de preliminar/Active, secundário/apoio a preliminar/apoio, secundário/Active

Solução:

Etapa 1. Clique sobre o ícone segundo as indicações da imagem.

Etapa 2. Confirme a ação na janela pop-up segundo as indicações da imagem.



Etapa 3. Verifique o resultado segundo as indicações da imagem.

Da LINA CLI, você pode ver que o comando no failover ative **esteve executado no preliminar/unidade ativa:**

```
Jul 22 2016 10:39:26: %ASA-5-111008: User 'enable_15' executed the 'no failover active' command.
Jul 22 2016 10:39:26: %ASA-5-111010: User 'enable_15', running 'N/A' from IP 0.0.0.0, executed
'no failover active'
```

Você pode igualmente verificá-lo no **comando history do Failover da mostra** output:

```
firepower# show failover history
==========================================================================
From State                  To State                    Reason
10:39:26 EEST Jul 22 2016
Active                      Standby Ready               Set by the config command
```

Etapa 4. Após a verificação, faça o Active da unidade primária outra vez.

Encarregue 5. pares de quebra HA

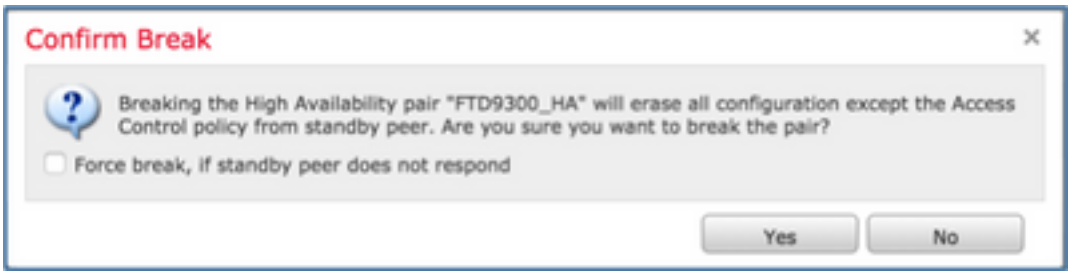
Exigência da tarefa:

Do FMC, quebre o par de failover.

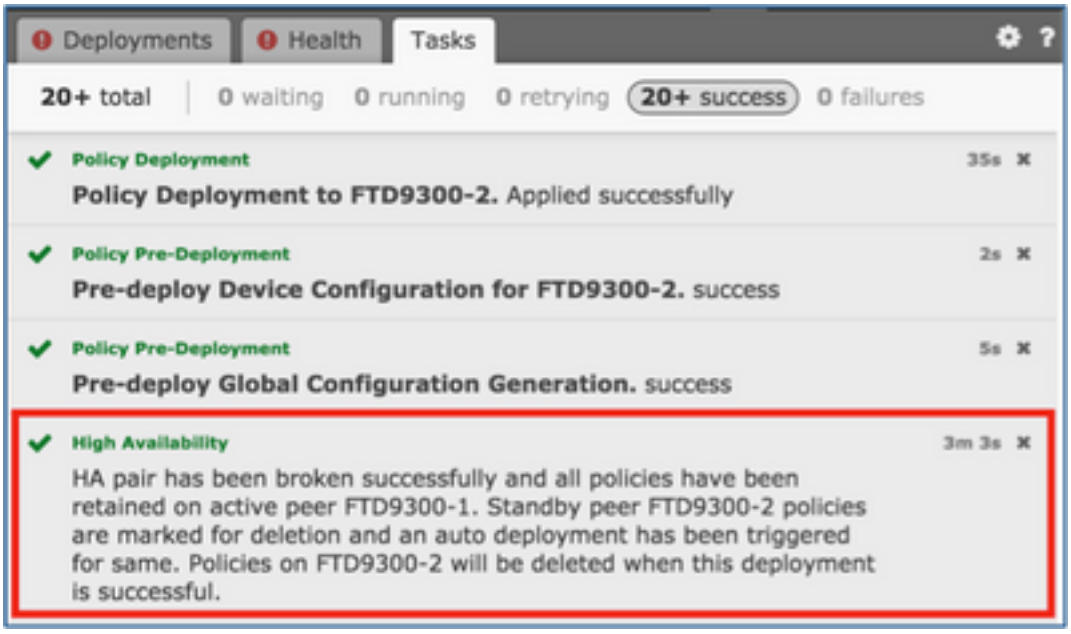
Solução:

Etapa 1. Clique sobre o ícone segundo as indicações da imagem.

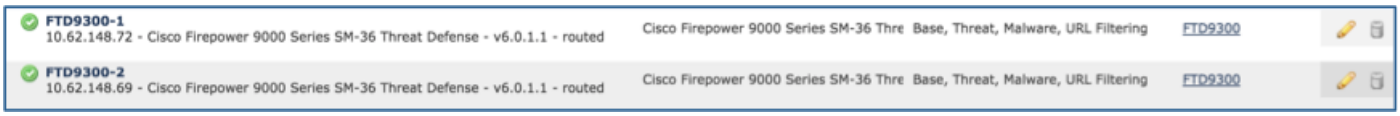
Etapa 2. Verifique a notificação segundo as indicações da imagem.



Etapa 3. Note a mensagem segundo as indicações da imagem.



Etapa 4. Verifique o resultado do FMC GUI segundo as indicações da imagem.



mostre a executar-configuração na unidade primária antes e depois de quebrar o HA:

Antes da ruptura HA

```
sh run do firepower#
: Salvar
:
: Número de série: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB RAM, E5 Series CPU
Xeon 2294 megahertz, 2 CPU (72 núcleos)
:
Versão 6.0.1.1 NGFW
!
hostname firePOWER
permita a senha 8Ry2YjIyt7RRXU24 cifrada
nomes
!
relação Ethernet1/2
Gerenciamento-somente
diagnóstico do nameif
nível de segurança 0
no ip address
!
relação Ethernet1/4
relação do Failover da descrição LAN/STATE
!
relação Ethernet1/5
nameif para dentro
nível de segurança 0
apoio 192.168.75.11 de 255.255.255.0 do endereço IP
192.168.75.10
!
relação Ethernet1/6
nameif fora
nível de segurança 0
apoio 192.168.76.11 de 255.255.255.0 do endereço IP
192.168.76.10
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observação da lista de
acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 -
Mandatory/1
regra-identificação 268447744 da observação da lista de
acesso CSM_FW_ACL_: REGRA L4: Allow_ICMP
ICMP avançado CSM_FW_ACL_ da licença da lista de acesso
algum algum regra-identificação 268447744 log de eventos
ambos
regra-identificação 268441600 da observação da lista de
```

Após a ruptura HA

```
sh run do firepower#
: Salvar
:
: Número de série: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB
Xeon 2294 megahertz, 2 CPU (72 núcleo
:
Versão 6.0.1.1 NGFW
!
hostname firePOWER
permita a senha 8Ry2YjIyt7RRXU24 cifra
nomes
!
relação Ethernet1/2
Gerenciamento-somente
diagnóstico do nameif
nível de segurança 0
no ip address
!
relação Ethernet1/4
nenhum nameif
nenhum nível de segurança
no ip address
!
relação Ethernet1/5
nameif para dentro
nível de segurança 0
apoio 192.168.75.11 de 255.255.255.0 d
192.168.75.10
!
relação Ethernet1/6
nameif fora
nível de segurança 0
apoio 192.168.76.11 de 255.255.255.0 d
192.168.76.10
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observ
acesso CSM_FW_ACL_: POLÍTICA DE A
Mandatory/1
regra-identificação 268447744 da observ
acesso CSM_FW_ACL_: REGRA L4: Allo
ICMP avançado CSM_FW_ACL_ da licen
algum algum regra-identificação 268447
```

acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 - Default/1
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_: REGRA L4: REGRA DA AÇÃO PADRÃO
licença avançada CSM_FW_ACL_ IP da lista de acesso alguma alguma regra-identificação 268441600
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
registrar permite
logging timestamp
apoio de registro
tamanho de buffer de registro 100000
logging buffered debugging
registrando 1024 flash-mínimo-livres
flash-máximo-atribuição de registro 3076
diagnóstico 1500 MTU
MTU dentro de 1500
MTU fora de 1500
Failover
unidade lan do Failover preliminar
fover_link Ethernet1/4 da relação lan do Failover
HTTP da replicação do Failover
MAC address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222 do Failover
MAC address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444 do Failover
fover_link Ethernet1/4 do link failover
apoio 1.1.1.2 de 1.1.1.1 255.255.255.0 do fover_link da relação IP do Failover
tamanho de intermitência 1 do taxa-limite 1 do ICMP não alcançável
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:00 UDP 0:02:00
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05:00 do sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 do intervalo
o sip_media 0:02:00 do sorvo 0:30:00 do intervalo sorvo-convida a sorvo-disconexão 0:02:00 de 0:03:00
absolute do uauth 0:05:00 dos sorvo-provisório-media 0:02:00 do intervalo
TCP-proxy-remontagem 0:00:30 do intervalo
intervalo flutuar-CONN 0:00:00
ambos
regra-identificação 268441600 da observ
acesso CSM_FW_ACL_: POLÍTICA DE A
Default/1
regra-identificação 268441600 da observ
acesso CSM_FW_ACL_: REGRA L4: RE
PADRÃO
licença avançada CSM_FW_ACL_ IP da
alguma alguma regra-identificação 2684
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
registrar permite
logging timestamp
apoio de registro
tamanho de buffer de registro 100000
logging buffered debugging
registrando 1024 flash-mínimo-livres
flash-máximo-atribuição de registro 3076
diagnóstico 1500 MTU
MTU dentro de 1500
MTU fora de 1500
sem falha
nenhum módulo de serviço da monitor-re
tamanho de intermitência 1 do taxa-limite
alcançável
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:0
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05
0:10:00 h323 0:05:00 h225 1:00:00 do int
o sip_media 0:02:00 do sorvo 0:30:00 do
convida a sorvo-disconexão 0:02:00 de 0
absolute do uauth 0:05:00 dos sorvo-prov
do intervalo
TCP-proxy-remontagem 0:00:30 do interv
intervalo flutuar-CONN 0:00:00
desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilha
autenticação que SNMP desativa o link o
inicialização lenta
PMTU-envelhecimento cripto da associaç

desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilhas a associação da autenticação que SNMP desativa o link o warmstart da inicialização lenta
PMTU-envelhecimento cripto da associação de segurança IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de chave do ssh
intervalo 0 do console
dinâmico-acesso-política-registro DfltAccessPolicy
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o preset_dns_map dns parâmetros
automóvel do cliente máximo do tamanho da mensagem
message-length maximum 512
o tipo do mapa de política inspeciona as IP-opções UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225
inspecione os ras h323
inspecione o rsh
inspecione o rtsp
inspecione o sqlnet
inspecione magro
inspecione o sunrpc
inspecione o xdmcp
inspecione o sorvo
inspecione o NetBIOS
inspecione tftp
inspecione o ICMP
inspecione o erro ICMP
inspecione o dcerpc
inspecione as IP-opções UM_STATIC_IP_OPTIONS_MAP
class class-default
ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão
!
IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de cha
intervalo 0 do console
dinâmico-acesso-política-registro DfltAcc
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o p
parâmetros
automóvel do cliente máximo do tamanho
message-length maximum 512
o tipo do mapa de política inspeciona as
UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225
inspecione os ras h323
inspecione o rsh
inspecione o rtsp
inspecione o sqlnet
inspecione magro
inspecione o sunrpc
inspecione o xdmcp
inspecione o sorvo
inspecione o NetBIOS
inspecione tftp
inspecione o ICMP
inspecione o erro ICMP
inspecione o dcerpc
inspecione as IP-opções UM_STATIC_IP
class class-default
ajuste as avançado-opções UM_STATIC_
conexão
!
service-policy global_policy global
contexto alerta do hostname
call-home
perfil CiscoTAC-1
não ativo
HTTP
https://tools.cisco.com/its/service/oddce/s

service-policy global_policy global
contexto alerta do hostname
call-home
perfil CiscoTAC-1
não ativo
HTTP
https://tools.cisco.com/its/service/oddce/services/DDCEService
do endereço de destino
email callhome@cisco.com do endereço de destino
HTTP do transporte-método do destino
diagnóstico do subscrever-à-alerta-grupo
ambiente do subscrever-à-alerta-grupo
revista mensal periódica do inventário do subscrever-à-alerta-grupo
revista mensal periódica da configuração do subscrever-à-alerta-grupo
diário periódico da telemetria do subscrever-à-alerta-grupo
Cryptochecksum:933c594fc0264082edc0f24bad358031
: fim
firepower#

do endereço de destino
email callhome@cisco.com do endereço
HTTP do transporte-método do destino
diagnóstico do subscrever-à-alerta-grupo
ambiente do subscrever-à-alerta-grupo
revista mensal periódica do inventário do
grupo
revista mensal periódica da configuração
alerta-grupo
diário periódico da telemetria do subscrev
Cryptochecksum:fb6f5c369dee730b9125
: fim
firepower#

a executar-configuração da mostra na unidade secundária antes e depois de quebrar o HA está segundo as indicações da tabela aqui.

Antes da ruptura HA	Após a ruptura HA
sh run do firepower#	sh run do firepower#
: Salvar	: Salvar
:	:
: Número de série: FLM19206H7T	: Número de série: FLM19206H7T
: Hardware: FPR9K-SM-36, 135841 MB RAM, E5 Series CPU Xeon 2294 megahertz, 2 CPU (72 núcleos)	: Hardware: FPR9K-SM-36, 135841 MB Xeon 2294 megahertz, 2 CPU (72 núcleo
:	:
Versão 6.0.1.1 NGFW	Versão 6.0.1.1 NGFW
!	!
hostname firePOWER	hostname firePOWER
permita a senha 8Ry2YjIyt7RRXU24 cifrada	permita a senha 8Ry2YjIyt7RRXU24 cifra
nomes	nomes
!	!
relação Ethernet1/2	relação Ethernet1/2
Gerenciamento-somente	Gerenciamento-somente
diagnóstico do nameif	diagnóstico do nameif
nível de segurança 0	nível de segurança 0
no ip address	no ip address
!	!
relação Ethernet1/4	**relação Ethernet1/4**
relação do Failover da descrição LAN/STATE	**fechamento**
!	**nenhum nameif**
relação Ethernet1/5	**nenhum nível de segurança**
nameif para dentro	**no ip address**
nível de segurança 0	**!**
apoio 192.168.75.11 de 255.255.255.0 do endereço IP 192.168.75.10	**relação Ethernet1/5**
!	**fechamento**
	nenhum nameif

relação Ethernet1/6
nameif fora
nível de segurança 0
apoio 192.168.76.11 de 255.255.255.0 do endereço IP 192.168.76.10
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 - Mandatory/1
regra-identificação 268447744 da observação da lista de acesso CSM_FW_ACL_: REGRA L4: Allow_ICMP
ICMP avançado CSM_FW_ACL_ da licença da lista de acesso algum algum regra-identificação 268447744 log de eventos ambos
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 - Default/1
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_: REGRA L4: REGRA DA AÇÃO PADRÃO
licença avançada CSM_FW_ACL_ IP da lista de acesso alguma alguma regra-identificação 268441600
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
registrar permite
logging timestamp
apoio de registro
tamanho de buffer de registro 100000
logging buffered debugging
registrando 1024 flash-mínimo-livres
flash-máximo-atribuição de registro 3076
diagnóstico 1500 MTU
MTU dentro de 1500
MTU fora de 1500
Failover
unidade lan do Failover secundária
fover_link Ethernet1/4 da relação lan do Failover
HTTP da replicação do Failover
MAC address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222 do Failover
MAC address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444 do Failover
fover_link Ethernet1/4 do link failover
apoio 1.1.1.2 de 1.1.1.1 255.255.255.0 do fover_link da relação IP do Failover
tamanho de intermitência 1 do taxa-limite 1 do ICMP não
nenhum nível de segurança
no ip address
!
relação Ethernet1/6
fechamento
nenhum nameif
nenhum nível de segurança
no ip address
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observ
acesso CSM_FW_ACL_: POLÍTICA DE A
Mandatory/1
regra-identificação 268447744 da observ
acesso CSM_FW_ACL_: REGRA L4: Allo
ICMP avançado CSM_FW_ACL_ da licen
algum algum regra-identificação 2684477
ambos
regra-identificação 268441600 da observ
acesso CSM_FW_ACL_: POLÍTICA DE A
Default/1
regra-identificação 268441600 da observ
acesso CSM_FW_ACL_: REGRA L4: RE
PADRÃO
licença avançada CSM_FW_ACL_ IP da
alguma alguma regra-identificação 26844
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
nenhum mensagem de registro 106015
nenhum mensagem de registro 313001
nenhum mensagem de registro 313008
nenhum mensagem de registro 106023
nenhum mensagem de registro 710003
nenhum mensagem de registro 106100
nenhum mensagem de registro 302015
nenhum mensagem de registro 302014
nenhum mensagem de registro 302013
nenhum mensagem de registro 302018
nenhum mensagem de registro 302017
nenhum mensagem de registro 302016
nenhum mensagem de registro 302021
nenhum mensagem de registro 302020
diagnóstico 1500 MTU
sem falha
nenhum módulo de serviço da monitor-re
tamanho de intermitência 1 do taxa-limite
alcançável

```
alcançável
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:00 UDP 0:02:00
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05:00 do sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 do intervalo
o sip_media 0:02:00 do sorvo 0:30:00 do intervalo sorvo-
convida a sorvo-disconexão 0:02:00 de 0:03:00
absolute do uauth 0:05:00 dos sorvo-provisório-media 0:02:00
do intervalo
TCP-proxy-remontagem 0:00:30 do intervalo
intervalo flutuar-CONN 0:00:00
LOCAL do domínio padrão da USER-identidade
desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilhas a associação da
autenticação que SNMP desativa o link o warmstart da
inicialização lenta
PMTU-envelhecimento cripto da associação de segurança
IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de chave do ssh
intervalo 0 do console
dinâmico-acesso-política-registro DfltAccessPolicy
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o preset_dns_map dns
parâmetros
automóvel do cliente máximo do tamanho da mensagem
message-length maximum 512
o tipo do mapa de política inspeciona as IP-opções
UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225
```

```
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:00
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05
0:10:00 h323 0:05:00 h225 1:00:00 do int
o sip_media 0:02:00 do sorvo 0:30:00 do
convida a sorvo-disconexão 0:02:00 de 0
absolute do uauth 0:05:00 dos sorvo-prov
do intervalo
TCP-proxy-remontagem 0:00:30 do interv
intervalo flutuar-CONN 0:00:00
desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilha
autenticação que SNMP desativa o link o
inicialização lenta
PMTU-envelhecimento cripto da associaç
IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de chav
intervalo 0 do console
dinâmico-acesso-política-registro DfltAcc
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o p
parâmetros
automóvel do cliente máximo do tamanho
message-length maximum 512
o tipo do mapa de política inspeciona as
UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225
inspecione os ras h323
inspecione o rsh
```

inspecione os ras h323
inspecione o rsh
inspecione o rtsp
inspecione o sqlnet
inspecione magro
inspecione o sunrpc
inspecione o xdmcp
inspecione o sorvo
inspecione o NetBIOS
inspecione tftp
inspecione o ICMP
inspecione o erro ICMP
inspecione o dcerpc
inspecione as IP-opções UM_STATIC_IP_OPTIONS_MAP
class class-default
ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão
!
service-policy global_policy global
contexto alerta do hostname
call-home
perfil CiscoTAC-1
não ativo
HTTP https://tools.cisco.com/its/service/oddce/services/DDCEService do endereço de destino
email callhome@cisco.com do endereço de destino
HTTP do transporte-método do destino
diagnóstico do subscrever-à-alerta-grupo
ambiente do subscrever-à-alerta-grupo
revista mensal periódica do inventário do subscrever-à-alerta-grupo
revista mensal periódica da configuração do subscrever-à-alerta-grupo
diário periódico da telemetria do subscrever-à-alerta-grupo
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84
: fim
firepower#

inspecione o rtsp
inspecione o sqlnet
inspecione magro
inspecione o sunrpc
inspecione o xdmcp
inspecione o sorvo
inspecione o NetBIOS
inspecione tftp
inspecione o ICMP
inspecione o erro ICMP
inspecione o dcerpc
inspecione as IP-opções UM_STATIC_IP
class class-default
ajuste as avançado-opções UM_STATIC_
conexão
!
service-policy global_policy global
contexto alerta do hostname
call-home
perfil CiscoTAC-1
não ativo
HTTP
https://tools.cisco.com/its/service/oddce/s
do endereço de destino
email callhome@cisco.com do endereço
HTTP do transporte-método do destino
diagnóstico do subscrever-à-alerta-grupo
ambiente do subscrever-à-alerta-grupo
revista mensal periódica do inventário do
grupo
revista mensal periódica da configuração
alerta-grupo
diário periódico da telemetria do subscrev
Cryptochecksum:08ed87194e9f5cd9149f
: fim
firepower#

Pontos principais a notar para quebrar o HA:

FTD preliminar	FTD secundário
Toda a configuração de failover é removida Os IP à espera permanecem	Toda a configuração é removida

Etapa 5. Depois que você termina esta tarefa, recreie os pares HA.

Pares do desabilitação HA da tarefa 6.

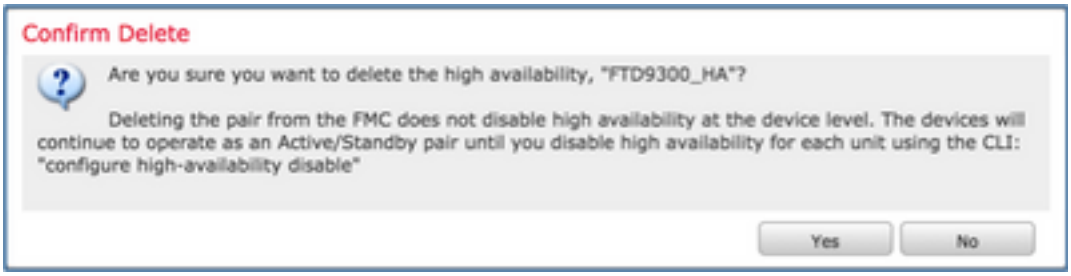
Exigência da tarefa:

Do FMC, desabilite o par de failover.

Solução:

Etapa 1. Clique sobre o ícone segundo as indicações da imagem.

Etapa 2. Verifique a notificação e confirme-a segundo as indicações da imagem.



Etapa 3. Depois que você suprime do HA, ambos os dispositivos estão removidos registro (removido) do FMC.

o resultado da executar-**configuração da mostra da** LINA CLI está segundo as indicações da tabela aqui:

Unidade primária	**Unidade secundária**
sh run do firepower#	sh run do firepower#
: Salvar	: Salvar
:	:
: Número de série: FLM19267A63	: Número de série: FLM19206H7T
: Hardware: FPR9K-SM-36, 135839 MB RAM, E5 Series CPU Xeon 2294 megahertz, 2 CPU (72 núcleos)	: Hardware: FPR9K-SM-36, 135841 MB Xeon 2294 megahertz, 2 CPU (72 núcleo
:	:
Versão 6.0.1.1 NGFW	Versão 6.0.1.1 NGFW
!	!
hostname firePOWER	hostname firePOWER
permita a senha 8Ry2YjIyt7RRXU24 cifrada	permita a senha 8Ry2YjIyt7RRXU24 cifra
nomes	nomes
!	!
relação Ethernet1/2	relação Ethernet1/2
Gerenciamento-somente	Gerenciamento-somente
diagnóstico do nameif	diagnóstico do nameif
nível de segurança 0	nível de segurança 0
no ip address	no ip address
!	!
relação Ethernet1/4	relação Ethernet1/4
relação do Failover da descrição LAN/STATE	relação do Failover da descrição LAN/ST
!	!
relação Ethernet1/5	relação Ethernet1/5
nameif para dentro	nameif para dentro
nível de segurança 0	nível de segurança 0
apoio 192.168.75.11 de 255.255.255.0 do endereço IP 192.168.75.10	**apoio 192.168.75.11 de 255.255.255.0 do 192.168.75.10**
!	!

relação Ethernet1/6
nameif fora
nível de segurança 0
apoio 192.168.76.11 de 255.255.255.0 do endereço IP 192.168.76.10
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 - Mandatory/1
regra-identificação 268447744 da observação da lista de acesso CSM_FW_ACL_: REGRA L4: Allow_ICMP
ICMP avançado CSM_FW_ACL_ da licença da lista de acesso algum algum regra-identificação 268447744 log de eventos ambos
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA DE ACESSO: FTD9300 - Default/1
regra-identificação 268441600 da observação da lista de acesso CSM_FW_ACL_: REGRA L4: REGRA DA AÇÃO PADRÃO
licença avançada CSM_FW_ACL_ IP da lista de acesso alguma alguma regra-identificação 268441600
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
registrar permite
logging timestamp
apoio de registro
tamanho de buffer de registro 100000
logging buffered debugging
registrando 1024 flash-mínimo-livres
flash-máximo-atribuição de registro 3076
diagnóstico 1500 MTU
MTU dentro de 1500
MTU fora de 1500
Failover
unidade lan do Failover preliminar
fover_link Ethernet1/4 da relação lan do Failover
HTTP da replicação do Failover
MAC address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222 do Failover
MAC address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444 do Failover
fover_link Ethernet1/4 do link failover
apoio 1.1.1.2 de 1.1.1.1 255.255.255.0 do fover_link da relação IP do Failover
tamanho de intermitência 1 do taxa-limite 1 do ICMP não

relação Ethernet1/6
nameif fora
nível de segurança 0
apoio 192.168.76.11 de 255.255.255.0 do
192.168.76.10
!
voz passiva do modo ftp
ID de VLAN do CONN-fósforo dos ngips
regra-identificação 268447744 da observa
acesso CSM_FW_ACL_: POLÍTICA DE A
Mandatory/1
regra-identificação 268447744 da observa
acesso CSM_FW_ACL_: REGRA L4: Allo
ICMP avançado CSM_FW_ACL_ da licen
algum algum regra-identificação 268447
ambos
regra-identificação 268441600 da observa
acesso CSM_FW_ACL_: POLÍTICA DE A
Default/1
regra-identificação 268441600 da observa
acesso CSM_FW_ACL_: REGRA L4: RE
PADRÃO
licença avançada CSM_FW_ACL_ IP da l
alguma alguma regra-identificação 26844
!
TCP-mapa UM_STATIC_TCP_MAP
a escala 6 7 das TCP-opções reserva
a escala 9 255 das TCP-opções reserva
a urgente-bandeira reserva
!
nenhum biper
registrar permite
logging timestamp
apoio de registro
tamanho de buffer de registro 100000
logging buffered debugging
registrando 1024 flash-mínimo-livres
flash-máximo-atribuição de registro 3076
diagnóstico 1500 MTU
MTU dentro de 1500
MTU fora de 1500
Failover
unidade lan do Failover secundária
fover_link Ethernet1/4 da relação lan do F
HTTP da replicação do Failover
MAC address Ethernet1/5 aaaa.bbbb.111
Failover
MAC address Ethernet1/6 aaaa.bbbb.333
Failover
fover_link Ethernet1/4 do link failover
apoio 1.1.1.2 de 1.1.1.1 255.255.255.0 do
relação IP do Failover
tamanho de intermitência 1 do taxa-limite

alcançável
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:00 UDP 0:02:00
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05:00 do sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 do intervalo
o sip_media 0:02:00 do sorvo 0:30:00 do intervalo sorvo-
convida a sorvo-disconexão 0:02:00 de 0:03:00
absolute do uauth 0:05:00 dos sorvo-provisório-media 0:02:00
do intervalo
TCP-proxy-remontagem 0:00:30 do intervalo
intervalo flutuar-CONN 0:00:00
desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilhas a associação da
autenticação que SNMP desativa o link o warmstart da
inicialização lenta
PMTU-envelhecimento cripto da associação de segurança
IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de chave do ssh
intervalo 0 do console
dinâmico-acesso-política-registro DfltAccessPolicy
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o preset_dns_map dns
parâmetros
automóvel do cliente máximo do tamanho da mensagem
message-length maximum 512
o tipo do mapa de política inspeciona as IP-opções
UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225
inspecione os ras h323

alcançável
nenhuma história do asdm permite
arp timeout 14400
nenhuma licença-nonconnected arp
acesso-grupo CSM_FW_ACL_ global
timeout xlate 3:00:00
pancadinha-xlate 0:00:30 do intervalo
ICMP entreaberto 0:00:02 do sctp 0:02:00
conexão 1:00:00 0:10:00 do intervalo
MGCP-pancadinha 0:05:00 do mgcp 0:05
0:10:00 h323 0:05:00 h225 1:00:00 do int
o sip_media 0:02:00 do sorvo 0:30:00 do
convida a sorvo-disconexão 0:02:00 de 0
absolute do uauth 0:05:00 dos sorvo-prov
do intervalo
TCP-proxy-remontagem 0:00:30 do interv
intervalo flutuar-CONN 0:00:00
LOCAL do domínio padrão da USER-iden
desabilitação do proxy-limite aaa
nenhum lugar do servidor snmp
nenhum contato do servidor snmp
nenhum servidor snmp permite armadilha
autenticação que SNMP desativa o link o
inicialização lenta
PMTU-envelhecimento cripto da associaç
IPSec infinito
política cripto do trustpool Ca
Timeout da Telnet 5
stricthostkeycheck do ssh
intervalo 5 do ssh
grupo dh-group1-sha1 das trocas de chav
intervalo 0 do console
dinâmico-acesso-política-registro DfltAcc
!
inspection_default do mapa de classe
padrão-inspeção-tráfego do fósforo
!
!
o tipo do mapa de política inspeciona o p
parâmetros
automóvel do cliente máximo do tamanho
message-length maximum 512
o tipo do mapa de política inspeciona as
UM_STATIC_IP_OPTIONS_MAP
parâmetros
a ação do eool reserva
a ação do nop reserva
a ação da alerta de roteador reserva
policy-map global_policy
inspection_default da classe
inspect dns preset_dns_map
inspecione o ftp
inspecione h323 h225

inspecione o rsh inspecione o rtsp inspecione o sqlnet inspecione magro inspecione o sunrpc inspecione o xdmcp inspecione o sorvo inspecione o NetBIOS inspecione tftp inspecione o ICMP inspecione o erro ICMP inspecione o dcerpc inspecione as IP-opções UM_STATIC_IP_OPTIONS_MAP class class-default ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão ! service-policy global_policy global contexto alerta do hostname call-home perfil CiscoTAC-1 não ativo HTTP https://tools.cisco.com/its/service/oddce/services/DDCEService do endereço de destino email callhome@cisco.com do endereço de destino HTTP do transporte-método do destino diagnóstico do subscrever-à-alerta-grupo ambiente do subscrever-à-alerta-grupo revista mensal periódica do inventário do subscrever-à-alerta-grupo revista mensal periódica da configuração do subscrever-à-alerta-grupo diário periódico da telemetria do subscrever-à-alerta-grupo Cryptochecksum:933c594fc0264082edc0f24bad358031 : fim firepower#	inspecione os ras h323 inspecione o rsh inspecione o rtsp inspecione o sqlnet inspecione magro inspecione o sunrpc inspecione o xdmcp inspecione o sorvo inspecione o NetBIOS inspecione tftp inspecione o ICMP inspecione o erro ICMP inspecione o dcerpc inspecione as IP-opções UM_STATIC_IP class class-default ajuste as avançado-opções UM_STATIC_ conexão ! service-policy global_policy global contexto alerta do hostname call-home perfil CiscoTAC-1 não ativo HTTP https://tools.cisco.com/its/service/oddce/s do endereço de destino email callhome@cisco.com do endereço HTTP do transporte-método do destino diagnóstico do subscrever-à-alerta-grupo ambiente do subscrever-à-alerta-grupo revista mensal periódica do inventário do grupo revista mensal periódica da configuração alerta-grupo diário periódico da telemetria do subscrev Cryptochecksum:e648f92dd7ef47ee611f2 : fim firepower#

Etapa 4. Ambos os dispositivos FTD foram removidos registro do FMC:

```
> show managers
No managers configured.
```

Etapa 5. Execute este comando remover a configuração de failover dos dispositivos FTD:

```
> configure high-availability disable
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO': yes
Successfully disabled high-availability.
```

Pontos principais a notar para desabilitar o HA:

FTD preliminar	FTD secundário

O dispositivo é removido do FMC. O dispositivo é removido do FMC.
Nenhuma configuração é removida do dispositivo FTD Nenhuma configuração é removida do dispositivo

Etapa 6. Depois que você termina a tarefa, registrar os dispositivos ao FMC e permita pares HA.

A tarefa 7. suspende o HA

Exigência da tarefa:

Suspenda o HA do FTD CLISH CLI

Solução:

Etapa 1. No FTD preliminar, execute o comando e confirme-o por **YE de** datilografia.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you
wish to abort: YES
Successfully suspended high-availability.
```

Etapa 2. Verifique as mudanças na unidade primária:

```
> show high-availability config
Failover Off
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Etapa 3. O resultado na unidade secundária:

```
> show high-availability config
Failover Off (pseudo-Standby)
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Etapa 4. Resumo HA na unidade primária:

```
> configure high-availability resume
Successfully resumed high-availablity.

> .
```

```
No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>

> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Etapa 5. O resultado na unidade secundária depois que você recomeça o HA:

```
> ..

Detected an Active mate
Beginning configuration replication from mate.


WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.

>

> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Todas as versões do manual de configuração do centro de gerenciamento de Cisco FirePOWER podem ser encontradas aqui

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Todas as versões dos guias do gerente e de configuração de CLI do chassi FXO podem ser encontradas aqui

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfId-121950

- O centro de assistência técnica (TAC) global de Cisco recomenda fortemente este guia visual para o conhecimento prático detalhado em tecnologias de segurança da próxima geração de Cisco FirePOWER, incluindo esses mencionados neste artigo.

http://www.ciscopress.com/title/9781587144806

- Para toda a configuração e TechNotes do Troubleshooting que se refere as Tecnologias de FirePOWER

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Suporte Técnico e Documentação - Cisco Systems