

Configurar várias instâncias no Secure Firewall 3100 Series

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar para a versão 7.4.1+](#)

Introdução

Este documento descreve como configurar a Multi-instância no Secure Firewall 3100 Series executando a versão 7.4+.

Pré-requisitos

Conhecimento do sistema operacional extensível (FXOS) de firewall e da interface gráfica do usuário (GUI) do Centro de gerenciamento de firewall (FMC).

Requisitos

Acesso a:

- Acesso do console ao Secure Firewall 3100 Series
- Acesso à GUI do FMC

Componentes Utilizados

- Cisco Secure Firewall Management Center executando a versão 7.4+
- Cisco Secure Firewall Series 3100
 - Exceto 3105*

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

No modo de várias instâncias, você pode implantar várias instâncias de contêiner em um único

chassi que atue como dispositivos completamente independentes.


Configurar para a versão 7.4.1+

Etapa 1. Conecte-se à porta de console do chassi.

A porta de console conecta-se à CLI FXOS.

Etapa 2. Faça login com o nome de usuário admin e a senha Admin123.

Você será solicitado a alterar a senha na primeira vez que fizer login no FXOS.

 Observação: se a senha já tiver sido alterada e você não a souber, será necessário recriar o dispositivo para redefinir a senha para o padrão. Consulte [o guia de Troubleshooting de FXOS](#) para obter [o procedimento de imagem](#).

Etapa 3. Verifique seu modo atual, Nativo ou Contêiner. Se o modo for Nativo, você poderá continuar com este procedimento para converter para o modo de várias instâncias (Contêiner).

```
firepower#show system detail
```

Exemplo:

```
firepower# show system detail

Systems:
  Name: firepower
  Mode: Stand Alone
  System IP Address: 0.0.0.0
  System IPv6 Address: ::
  System Owner:
  System Site:
  Deploy Mode: Native
  Description for System:
```

Mostrar estado de várias instâncias

Etapa 4. Conecte-se à CLI de defesa contra ameaças.

```
firepower# connect ftd
```

Exemplo:



```
firepower# connect ftd
>
```

Conectando ao FTD

Etapa 5. Na primeira vez que você fizer login na defesa contra ameaças, será solicitado que você aceite o Contrato de Licença de Usuário Final (EULA). O script de configuração da CLI é apresentado a você.

O script de configuração permite definir o endereço IP da interface de gerenciamento e outras configurações. No entanto, quando você converte para o modo de várias instâncias, as únicas configurações mantidas são as seguintes.

- Senha do administrador (definida no login inicial)
- Servidores DNS
- Pesquisar domínios

Você redefine o gateway e o endereço IP de gerenciamento como parte do comando do modo de várias instâncias. Depois de converter para o modo de várias instâncias, você pode alterar as configurações de Gerenciamento na CLI FXOS. [Consulte Alterar as configurações de gerenciamento do chassi na CLI do FXOS.](#)

Etapa 6. Ative o modo de várias instâncias, defina as configurações da interface de gerenciamento do chassi e identifique o centro de gerenciamento. Você pode usar IPv4 e/ou IPv6. Depois de inserir o comando, você será solicitado a apagar a configuração e reinicializar. Digite ERASE(todas em maiúsculas). O sistema é reinicializado e, como parte da alteração do modo, apaga a configuração, com exceção das configurações de rede de gerenciamento definidas no comando e da senha admin. O nome de host do chassi está definido como "modelo firepower".

IPv4:

configurar rede de várias instâncias

```
ipv4ip_addressnetwork_maskgateway_ip_addressmanagermanager_name  
{hostname | ipv4_address | DONTRESOLVE} registration_keynat_id
```

IPv6:

configure a rede de várias instâncias

```
ipv6ipv6_addressprefix_lengthgateway_ip_addressmanagermanager_name  
{hostname | ipv6_address | DONTRESOLVE} registration_keynat_id
```

Consulte estes componentes do gerenciador:


- {hostname | ipv4_address | DONTRESOLVE} —Especifica o FQDN ou o endereço IP do centro de gerenciamento. Pelo menos um dos dispositivos, o centro de gerenciamento ou o chassi, deve ter um endereço IP acessível para estabelecer o canal de comunicação bidirecional criptografado SSL entre os dois dispositivos. Se você não especificar um nome de host ou endereço IP de gerenciador nesse comando, insiraDONTRESOLVE; nesse caso, o chassi deve ter um endereço IP ou nome de host acessível e você deve especificar thenat_id.
- registration_key — insira uma chave de registro única de sua escolha que você também deve especificar no centro de gerenciamento ao registrar o chassi. A chave de registro não deve exceder 37 caracteres. Os caracteres válidos incluem caracteres alfanuméricos (A-Z, a-z, 0-9) e o hífen (-).
- nat_id — Especifica uma string única e exclusiva de sua escolha que você também especifica no centro de gerenciamento quando você registra o chassi quando um lado não especifica um endereço IP ou nome de host acessível. É obrigatório se você não especificar um endereço de gerenciador ou nome de host, no entanto, recomendamos que você sempre defina a ID de NAT mesmo quando especificar um nome de host ou endereço IP. A ID do NAT não deve exceder 37 caracteres. Os caracteres válidos incluem caracteres alfanuméricos (A-Z, a-z, 0-9) e o hífen (-). Essa ID não pode ser usada para nenhum outro dispositivo registrado no centro de gerenciamento.


Para alterar o modo de volta para o modo de dispositivo, você deve usar o sistema FXOS CLI e enterscope e set deploymode native. [Consulte Alterar as configurações de gerenciamento do chassi na CLI do FXOS.](#)

Exemplo:

```
> configure multi-instance network ipv4 10.88.146.203 255.255.255.0 10.88.146.1  
manager fmc1 10.88.243.100 cisco123 natid1  
WARNING: This command will discard any FTD configuration (except admin's credentials). Make sure you backup your content  
. All previous content will be lost. System is going to be re-initialized. Type ERASE to confirm:ERASE  
Continue...  
Validation check...  
Checking startup version and csp file ...  
Converting to MI mode, device will be rebooted and re-initialized...  
>  
Broadcast message from root@firepower (Sun Jan 22 00:10:14 2023):  
  
All shells being terminated due to system /sbin/reboot  
  
Broadcast message from root@firepower (Sun Jan 22 00:10:15 2023):  
  
System is restarted due to deploy mode changed
```

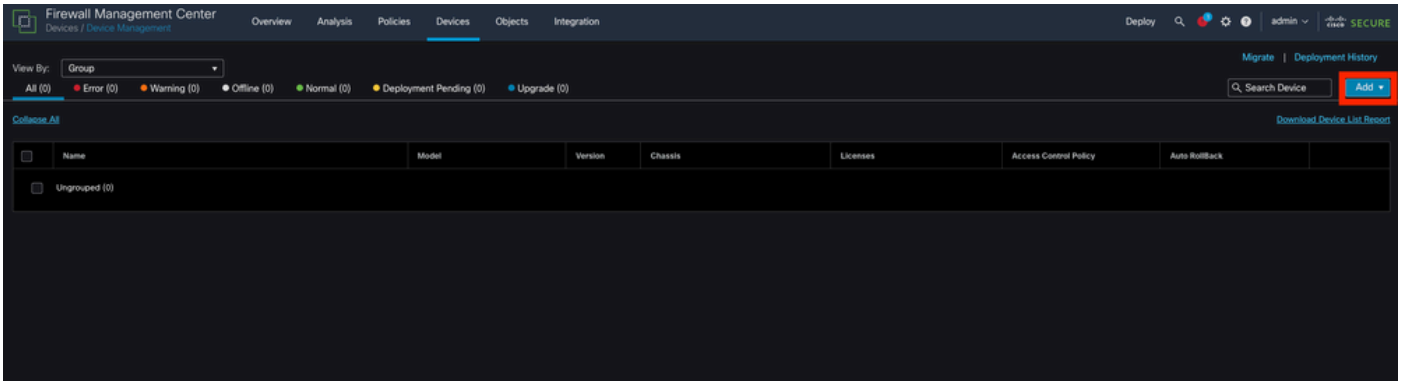
Alterando para o Modo de Várias Instâncias

 Observação: adicione o chassi de várias instâncias ao centro de gerenciamento. O centro de gerenciamento e o chassi compartilham uma conexão de gerenciamento separada

 usando a interface de gerenciamento do chassi. Você pode usar o centro de gerenciamento para definir todas as configurações de chassi, bem como instâncias. Não há suporte para o gerenciador de chassis do Secure Firewall ou para a configuração na CLI FXOS.

Passo 7. No centro de gerenciamento, adicione o chassi usando o endereço IP ou o nome do host de gerenciamento do chassi.

- Selecione Devices>Device Management e, em seguida, Add>Chassis.



Adição do chassi ao FMC

Add Chassis



i This operation is only supported on 3100, 4100 & 9300 chassis

Hostname/IP Address†

Chassis name

Registration key*

Device Group

Unique NAT ID†

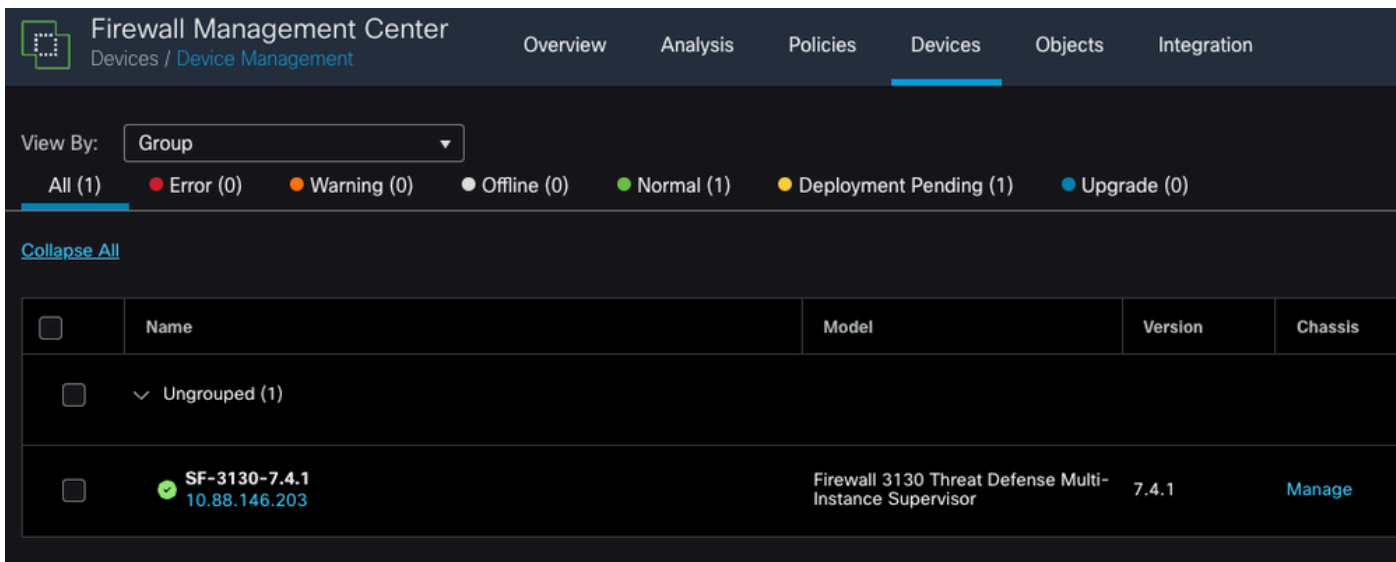
† Either host or NAT ID is required.

Cancel

Submit

Parâmetros de configuração do chassi

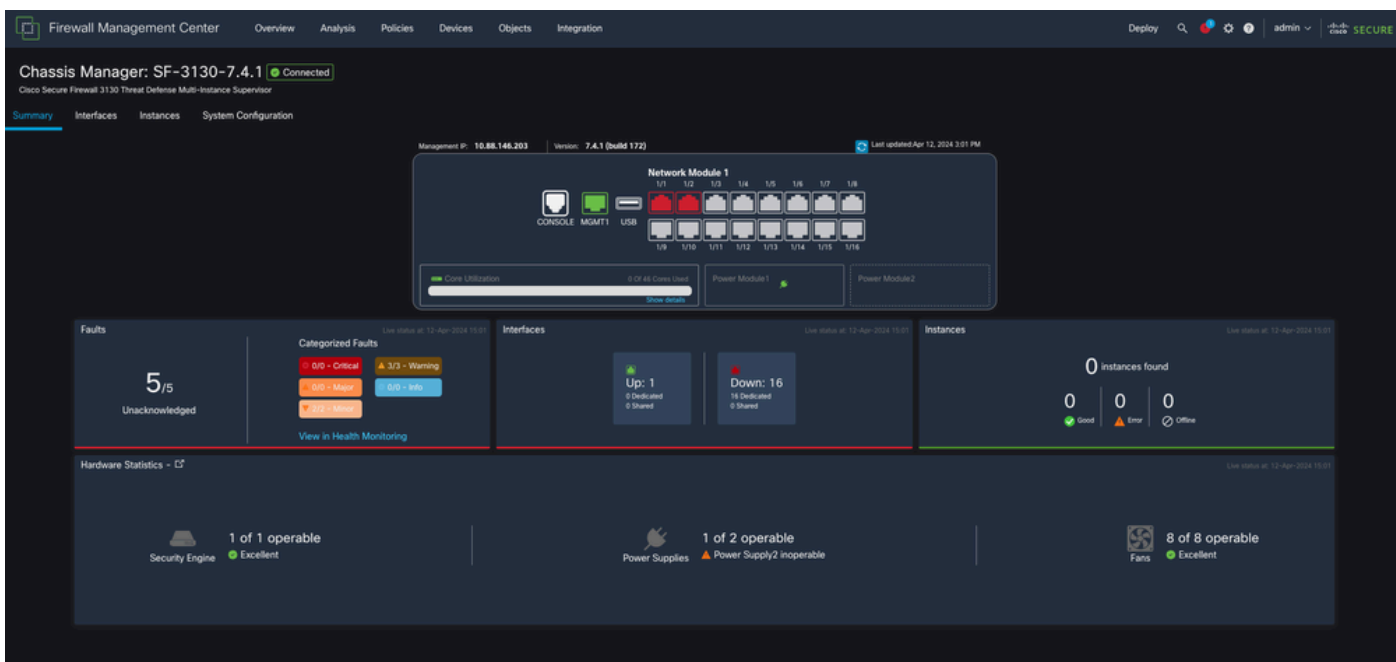
- Quando o chassi for adicionado ao FMC, consulte o dispositivo na lista de dispositivos no FMC.



Chassi adicionado ao FMC

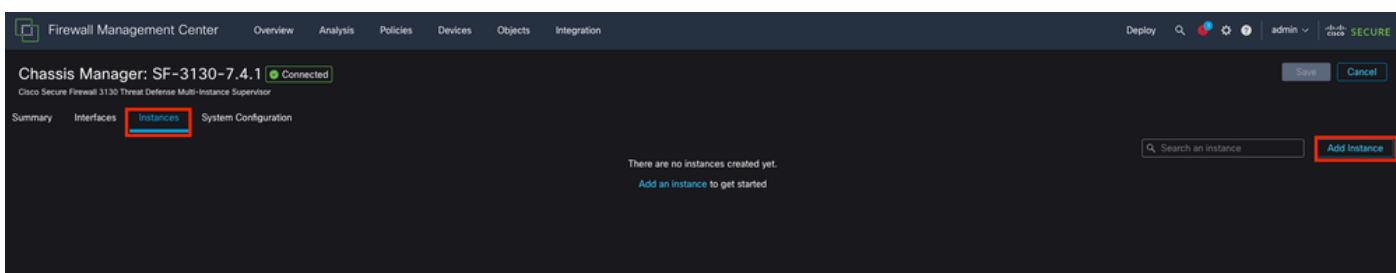
Etapa 8. Para exibir e configurar o chassi, clique em Gerenciar na coluna Chassi ou clique em Editar(✎).

A página Gerenciador de chassis é aberta para o chassi na página Resumo.



Gerenciamento de chassi

Etapa 9. Selecione o botão Instâncias e, em seguida, Adicionar instância para criar uma nova instância no chassi.



Etapa 10. Siga o assistente para concluir a instalação da Instância.

1. Aceite o contrato

Add Instance

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

End User License Agreement
Effective: May 10, 2022
Secure Firewall Terms and Conditions

By clicking 'Accept' below or using this Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and applicable Product Specific Terms available at:

<https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>

You also acknowledge that you have read the Cisco Privacy Statement at:

<https://www.cisco.com/c/en/us/about/legal/privacy-full.html>

If you are a Cisco partner accepting on behalf of an end customer, you must inform the end customer that the EULA applies to such end customer's use of the Cisco Technology and provide the end customer with access to all relevant terms. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'Accept' and do not use the Cisco Technology.

I understand and accept the agreement.

Cancel **Next**

Aceitar contrato

2. Configurar os parâmetros da Instância

Add Instance ? X

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Display Name*
SF-3130-741-Instance

Device Version*
7.4.1.172

Resource Profile*
Default-Medium +

Permit Expert mode for CLI

IPv4 IPv6 Both

IPv4

Management IP*
10.88.146.198

Network Mask*
255.255.255.0

Network Gateway*
10.88.146.1

Search Domain

FQDN

Firewall Mode*
Routed

DNS Servers
172.18.108.34

Device SSH Password*
.....

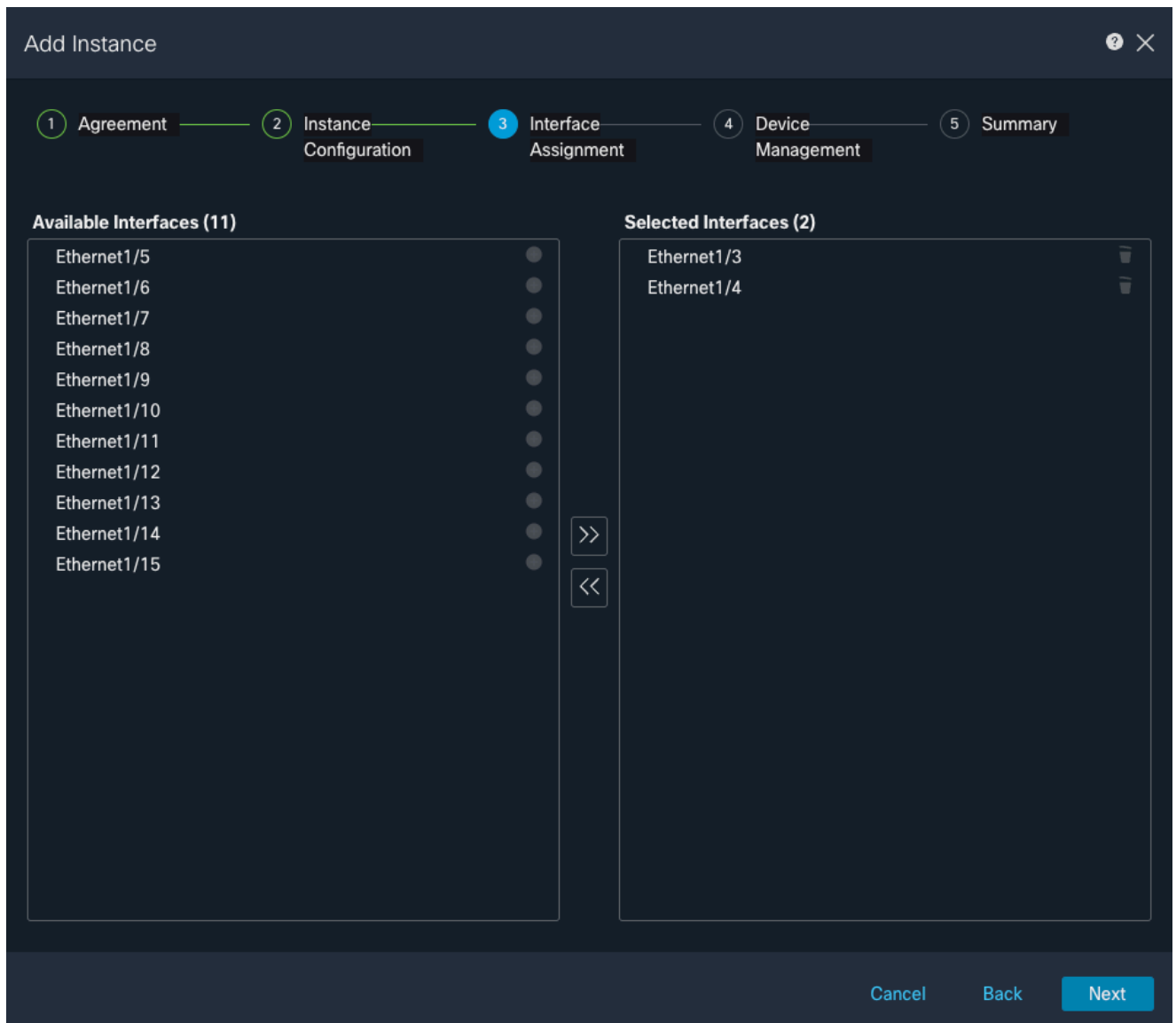
Confirm Password*
.....

Show Password

Cancel Back **Next**

Parâmetros de Instância

3. Interface Selection (Seleção de interface).



Atribuição de interface

4. Gerenciamento de dispositivos.

Add Instance ? ×

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Device Group
Select... ▾

Access Control Policy*
ACP ▾ +

Platform Settings
Instance x ▾ +

Smart Licensing

- Carrier
- Malware Defense
- IPS
- URL

Cancel Back Next

Gerenciamento de dispositivos

5. Summary

Add Instance



- 1 Agreement
- 2 Instance Configuration
- 3 Interface Assignment
- 4 Device Management
- 5 Summary

Instance Configuration

Name: asdvav
Version: 7.4.1.172
Resource Profile: Default-Small
IP: 10.88.243.13
Mask: 255.255.255.0
Gateway: 10.88.243.1
Mode: routed
Password: *****
FQDN:
DNS Servers:
Search Domain:
Expert Mode: disabled

Device Management - This info is required only during instance creation.

Access Policy: ACP
Device Group:
Platform Policy: Instance
Licenses: Carrier, Malware Defense, IPS, URL

Interface Assignment - 2 dedicated and 0 shared interfaces attached [Show All](#)

Cancel

Back

Save

Resumo da instância

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.