

Determine a versão ativa do Snort executada no Firepower Threat Defense (FTD)

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Determinar a Versão do Snort Ativo Executada no FTD](#)

[Interface de Linha de Comando \(CLI - Command Line Interface\) FTD](#)

[FTD Gerenciado pelo Cisco FDM](#)

[FTD Gerenciado pelo Cisco FMC](#)

[FTD Gerenciado pelo CDO da Cisco](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para confirmar a versão de snort ativa que um FTD da Cisco executa quando é gerenciado pelo FDM da Cisco, pelo FMC da Cisco ou pelo CDO.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower
- Gerenciador de dispositivos Cisco Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

Componentes Utilizados

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

- Defesa contra ameaças do Cisco Firepower v6.7.0 e 7.0.0
- Cisco Firepower Management Center v6.7.0 e 7.0.0
- Cisco Defense Orchestrator

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

O SNORT® Intrusion Prevention System lançou oficialmente o Snort 3, uma atualização abrangente que apresenta melhorias e novos recursos que melhoram o desempenho, processamento mais rápido, melhor escalabilidade para sua rede e uma variedade de mais de 200 plug-ins para que você possa criar uma configuração personalizada para sua rede.

As vantagens do Snort 3 incluem, entre outras:

- Melhor desempenho
- Inspeção SMBv2 aprimorada
- Novos recursos de detecção de script
- Inspeção HTTP/2
- Grupos de regras personalizados
- Sintaxe que facilita a gravação de regras de intrusão personalizadas.
- Motivos pelos quais ele teria deixado cair resultados em linha em eventos de invasão.
- O Snort não é reiniciado quando as alterações são implantadas no VDB, nas políticas SSL, nos detectores de aplicativos personalizados, nas fontes de identidade do portal cativo e na descoberta de identidade do servidor TLS.
- Maior facilidade de manutenção, devido aos dados de telemetria específicos do Snort 3 enviados para a Cisco Success Network e a melhores registros de solução de problemas.

O suporte para Snort 3.0 foi introduzido para o 6.7.0 Cisco Firepower Threat Defense (FTD), exatamente quando o FTD é gerenciado pelo Cisco Firepower Device Manager (FDM).

 Observação: para as novas implantações do FTD do 6.7.0 gerenciadas pelo FDM, o Snort 3.0 é o mecanismo de inspeção padrão. Se você atualizar o FTD para 6.7 a partir de uma versão mais antiga, o Snort 2.0 permanecerá o mecanismo de inspeção ativo, mas você poderá mudar para o Snort 3.0.

 Observação: para esta versão, o Snort 3.0 não suporta roteadores virtuais, regras de controle de acesso baseado em tempo ou a descriptografia de TLS 1.1 ou conexões inferiores. Habilite o Snort 3.0 somente se você não precisar desses recursos.

Em seguida, o Firepower versão 7.0 apresentou o suporte ao Snort 3.0 para os dispositivos Firepower Threat Defense gerenciados por ambos: o Cisco FDM e o Cisco Firepower

Management Center (FMC).

 Observação: para as novas implantações do FTD 7.0, o Snort 3 agora é o mecanismo de inspeção padrão. As implantações atualizadas continuam a usar o Snort 2, mas você pode alternar a qualquer momento.

 Cuidado: você pode alternar livremente entre o Snort 2.0 e o 3.0, para que possa reverter suas alterações, se necessário. O tráfego é interrompido sempre que você muda de versão.

 Cuidado: antes de alternar para o Snort 3, é altamente recomendável que você leia e compreenda o [Guia de configuração do Snort 3 do Firepower Management Center](#). Preste atenção especial às limitações de recursos e instruções de migração. Embora a atualização para o Snort 3 seja projetada para impacto mínimo, os recursos não mapeiam exatamente. O planejamento e a preparação antes da atualização podem ajudá-lo a garantir que o tráfego seja tratado conforme o esperado.

Determinar a Versão do Snort Ativo Executada no FTD

Interface de Linha de Comando (CLI - Command Line Interface) FTD

Para determinar a versão de snort ativa que é executada em um FTD, faça login na CLI do FTD e execute o comando `show snort3 status`:

Exemplo 1: quando não há saída exibida, o FTD executa o Snort 2.

```
<#root>  
>  
show snort3 status  
  
>
```

Exemplo 2: quando a saída mostrar, Atualmente executando Snort 2, o FTD executará Snort 2.

```
<#root>  
>  
show snort3 status
```

Currently running Snort 2

Exemplo 3: quando a saída mostrar, Atualmente executando Snort 3, o FTD executará Snort 3.

```
<#root>
```

```
>
```

```
show snort3 status
```

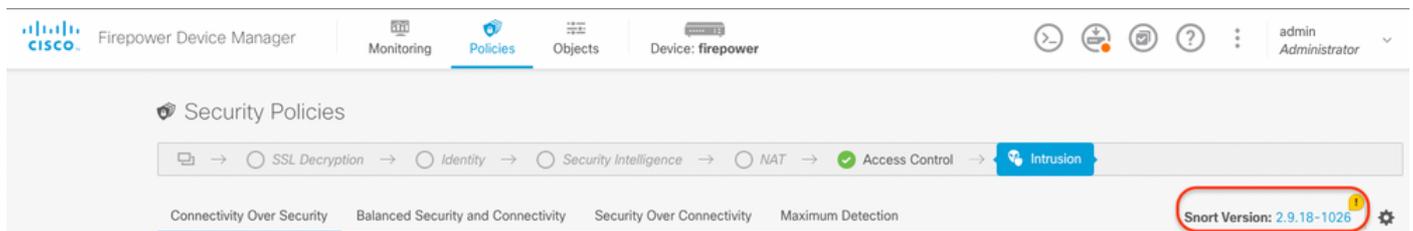
Currently running Snort 3

FTD Gerenciado pelo Cisco FDM

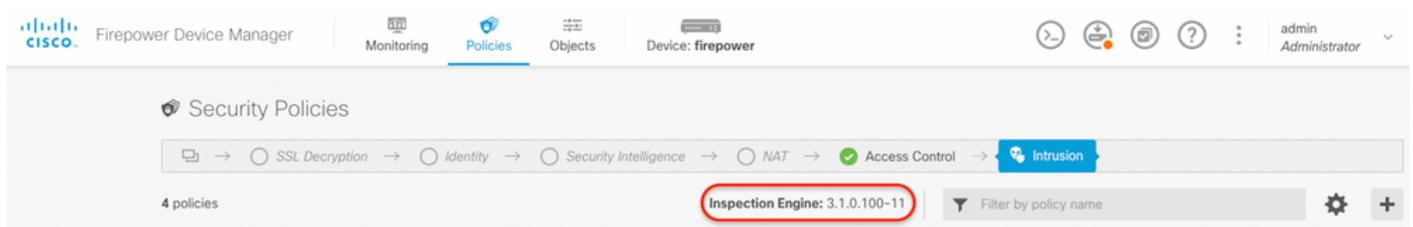
Para determinar a versão de snort ativa executada em um FTD gerenciado pelo Cisco FDM, siga as próximas etapas:

1. Faça login no Cisco FTD por meio da interface da Web do FDM.
2. No menu principal, selecione Policies.
3. Em seguida, selecione a guia Intrusion.
4. Procure a seção Snort Version ou Inspection Engine para confirmar a versão do Snort que está ativa no FTD.

Exemplo 1: o FTD executa a versão 2 do snort.



Exemplo 2: o FTD executa a versão 3 do snort.



FTD Gerenciado pelo Cisco FMC

Para determinar a versão de snort ativa executada em um FTD gerenciado pelo FMC da Cisco, siga as próximas etapas:

1. Faça login na interface da Web do Cisco FMC.
2. No menu Devices, selecione Device Management.
3. Em seguida, selecione o dispositivo FTD apropriado.
4. Clique no ícone do lápis Edit.

5. Selecione a guia Device e procure a seção Inspection Engine para confirmar a versão do snort que está ativa no FTD:

Exemplo 1: o FTD executa a versão 2 do snort.

The screenshot shows the Cisco Firepower Management Center interface for a device named vFTD-1. The 'Devices' tab is selected. The configuration is divided into several sections: General, License, System, Health, and Management. The 'Inspection Engine' section is highlighted with a red box and shows 'Inspection Engine: Snort 2'. Below this, a blue notification box titled 'NEW Upgrade to our new and improved Snort 3' provides information about the latest version, including a warning that switching snort versions requires a deployment and may cause traffic loss. The 'System' section shows the model as 'Cisco Firepower Threat Defense for VMware' and the version as '7.0.4'. The 'Health' section shows the status as 'Initial_Health_Policy 2018-02-28 14:46:00' and 'Excluded: None'. The 'Management' section shows the host and FMC Access Interface as 'Management Interface'.

Exemplo 2: o FTD executa a versão 3 do snort.

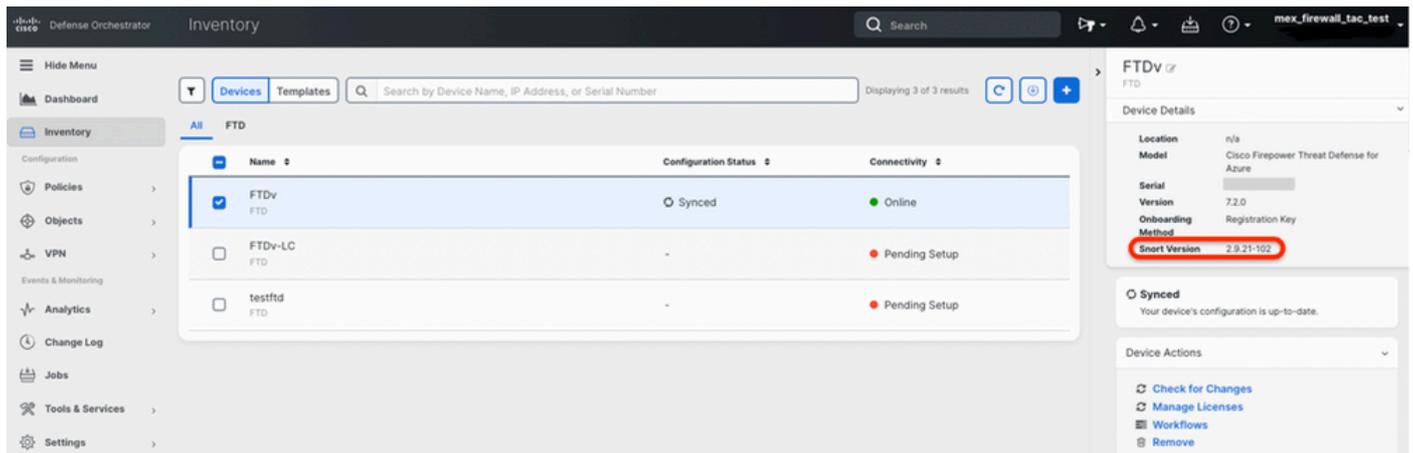
The screenshot shows the Cisco Firepower Management Center interface for a device named FTD1010-1. The 'Devices' tab is selected. The configuration is divided into several sections: General, License, System, Health, and Management. The 'Inspection Engine' section is highlighted with a red box and shows 'Inspection Engine: Snort 3'. Below this, a blue notification box titled 'significant improvements to performance and security efficacy, there is a lot to be excited about! Learn more' provides information about the latest version, including a warning that switching snort versions requires a deployment and may cause traffic loss. The 'System' section shows the model as 'Cisco Firepower 1010 Threat Defense' and the version as '7.0.4'. The 'Health' section shows the status as 'Initial_Health_Policy 2018-02-28 14:46:00' and 'Excluded: None'. The 'Management' section shows the host and FMC Access Interface as 'Management Interface'.

FTD Gerenciado pelo CDO da Cisco

Para determinar a versão de snort ativa que é executada em um FTD gerenciado pelo Cisco Defense Orchestrator, continue com as próximas etapas:

1. Faça login na interface da Web do Cisco Defense Orchestrator.
2. No menu Inventory, selecione o dispositivo FTD apropriado.
3. Na seção Device Details, procure Snort Version:

Exemplo 1: o FTD executa a versão 2 do snort.



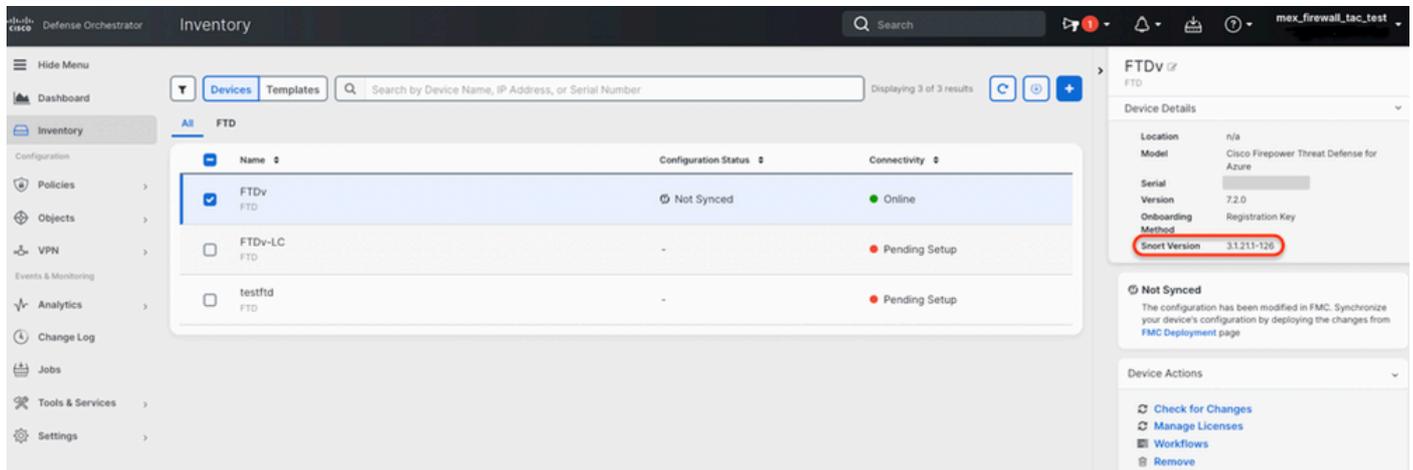
The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The 'Inventory' section is active, displaying a table of FTD devices. The 'FTDv' device is selected, and its details are shown on the right. The 'Snort Version' is highlighted in red, indicating it is 2.9.21-102.

Name	Configuration Status	Connectivity
FTDv FTD	Synced	Online
FTDv-LC FTD	-	Pending Setup
testftd FTD	-	Pending Setup

Device Details for FTDv:

- Location: n/a
- Model: Cisco Firepower Threat Defense for Azure
- Serial: [Redacted]
- Version: 7.2.0
- Onboarding Method: Registration Key
- Snort Version: 2.9.21-102

Exemplo 2: o FTD executa a versão 3 do snort.



The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The 'Inventory' section is active, displaying a table of FTD devices. The 'FTDv' device is selected, and its details are shown on the right. The 'Snort Version' is highlighted in red, indicating it is 3.1.21-120.

Name	Configuration Status	Connectivity
FTDv FTD	Not Synced	Online
FTDv-LC FTD	-	Pending Setup
testftd FTD	-	Pending Setup

Device Details for FTDv:

- Location: n/a
- Model: Cisco Firepower Threat Defense for Azure
- Serial: [Redacted]
- Version: 7.2.0
- Onboarding Method: Registration Key
- Snort Version: 3.1.21-120

Informações Relacionadas

- [Notas de versão do Cisco Firepower, versão 6.7.0](#)
- [Notas de versão do Cisco Firepower, versão 7.0](#)
- [Site do Snort 3](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.