

Atualizar do Snort 2 para o Snort 3 via FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como atualizar a versão do Snort 2 para o Snort 3 no Firepower Device Manager (FDM).

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- Firepower Device Manager (FDM)
- Snort.

Requisitos

Verifique se você tem os seguintes requisitos:

- Acesso ao Firepower Device Manager.
- Privilégios administrativos no FDM.
- O FTD deve ser pelo menos da versão 6.7 para usar o snort 3.

Componentes Utilizados

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

- FTD 7.2.7

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

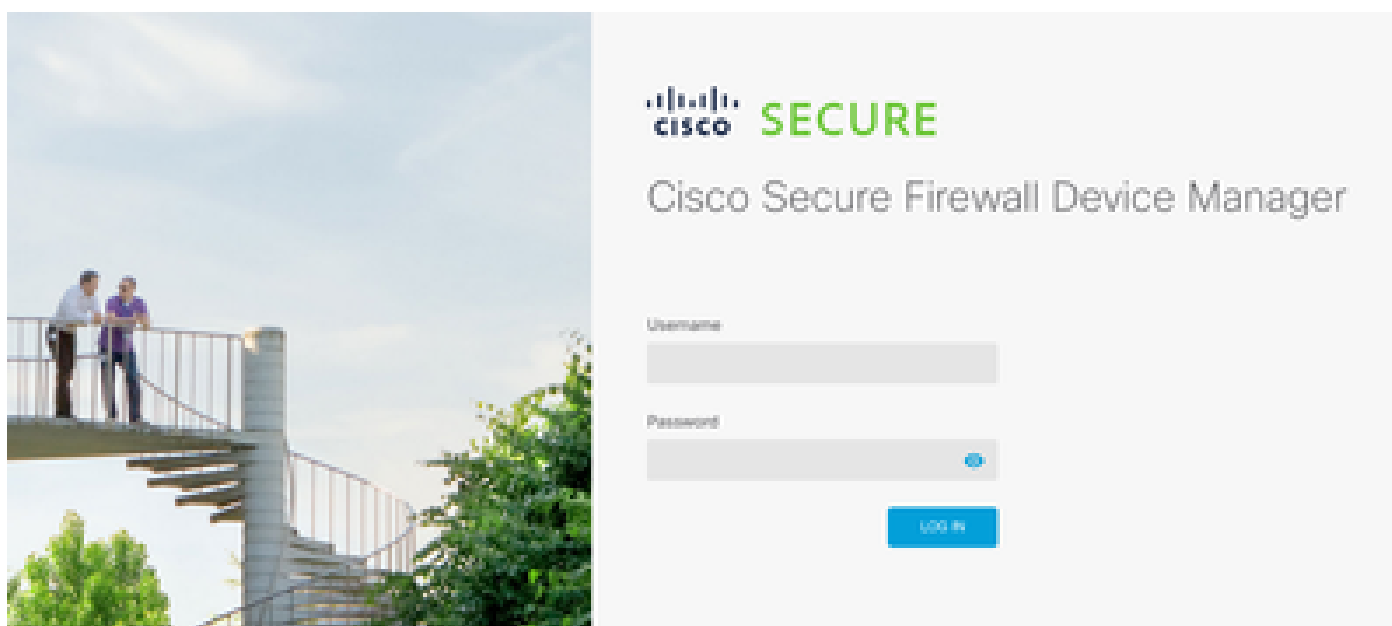
O recurso snort 3 foi adicionado na versão 6.7 do Firepower Device Manager (FDM). O Snort 3.0 foi projetado para lidar com estes desafios:

- Reduza o uso de memória e CPU.
- Melhorar a eficácia da inspeção HTTP.
- Carregamento mais rápido da configuração e reinicialização do snort.
- Melhor capacidade de programação para adição mais rápida de recursos.

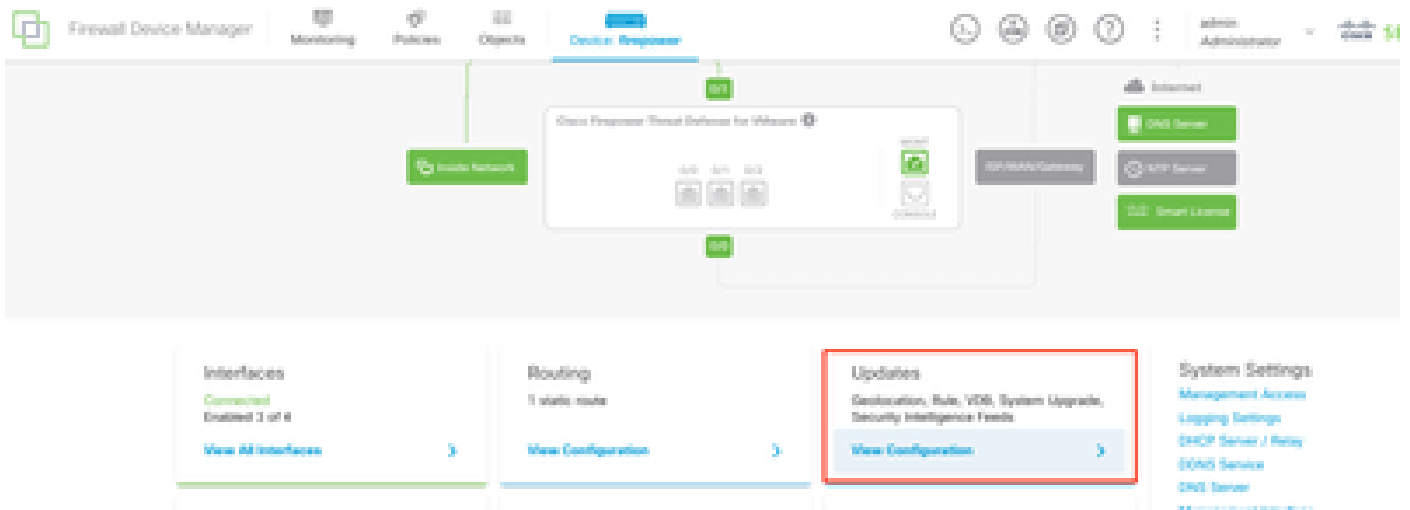
Configurar

Configurações

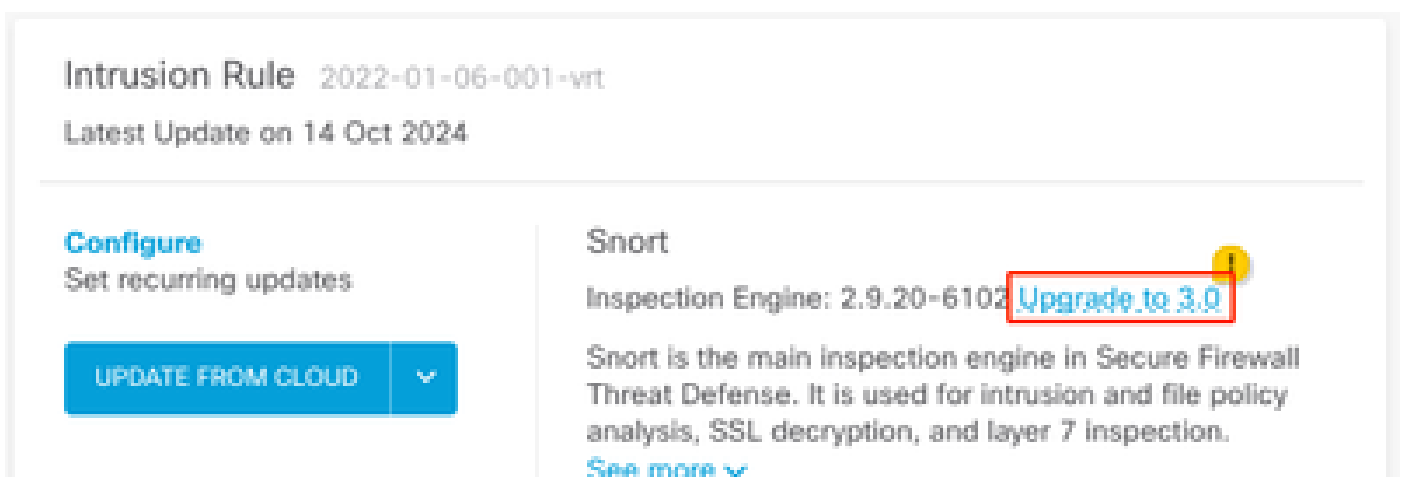
1. Faça logon no Gerenciador de dispositivos do Firepower.



2. Navegue até Device > Updates > View configuration.



3. Na seção regras de intrusão, clique em atualizar para o snort 3.



4. Na mensagem de aviso para confirmar sua seleção, selecione a opção para obter o pacote de regras de intrusão mais recente e clique em Sim.

Enable Snort 3.0



- Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
- The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive. We recommend that you start the switch at a time you will not need to use the device manager.



Get latest intrusion rules 

Are you sure you want to enable Snort 3.0?

NO

YES

Latest Update on 14 Oct 2024



Observação: o sistema baixa pacotes somente para a versão ativa do Snort, por isso é improvável que você tenha o pacote mais recente instalado para a versão do Snort para a qual você está mudando. Você deve aguardar até que a tarefa para alternar versões seja concluída para poder editar políticas de intrusão.



Aviso: a alternância da versão snort leva a uma perda momentânea de tráfego.

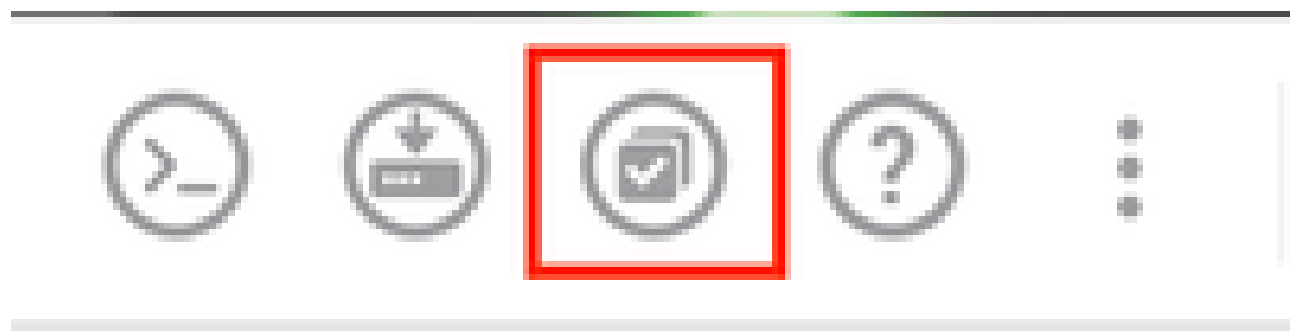
5. Você deve confirmar na lista de tarefas que a atualização foi iniciada.

Task List

18 total | 1 running | 13 completed | 4 failures [Delete all finished tasks](#)

Name	Start Time	End Time	Status	Actions
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM		Snort 3 Package Downloading in progress.	

Observação: a lista de tarefas está localizada na barra de navegação ao lado do ícone de disponibilizações.



Verificar

A seção Mecanismo de inspeção mostra que a versão atual do Snort é Snort 3.

Intrusion Rule 20241010-1555

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

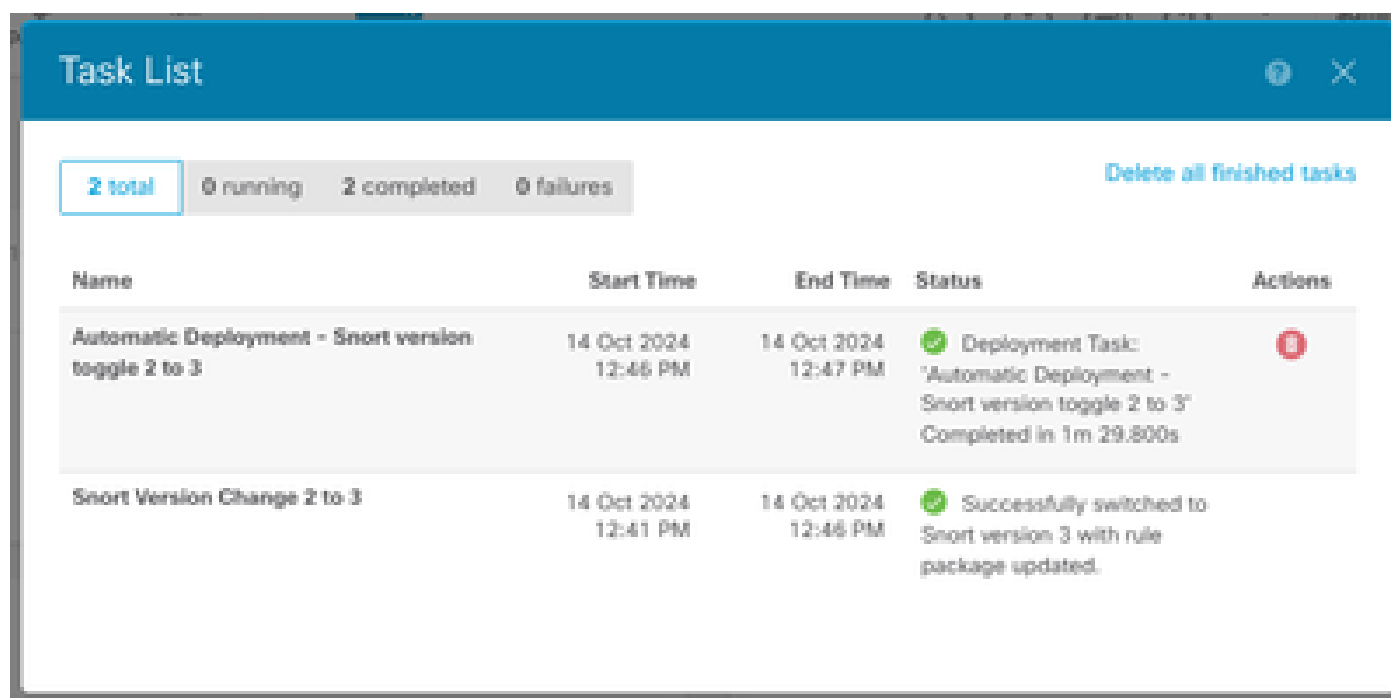
Snort

Inspection Engine: 3.1.21.600-26 [Downgrade to 2.9](#)

Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.

[See more](#)

Por fim, na lista de tarefas, certifique-se de que a alteração para snort 3 tenha sido concluída e implantada com êxito.



The screenshot shows a 'Task List' window with a blue header. Below the header, there are summary statistics: '2 total', '0 running', '2 completed', and '0 failures'. A 'Delete all finished tasks' link is visible on the right. The main content is a table with columns for Name, Start Time, End Time, Status, and Actions.

Name	Start Time	End Time	Status	Actions
Automatic Deployment - Snort version toggle 2 to 3	14 Oct 2024 12:46 PM	14 Oct 2024 12:47 PM	Deployment Task: 'Automatic Deployment - Snort version toggle 2 to 3' Completed in 1m 29.800s	
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM	14 Oct 2024 12:46 PM	Successfully switched to Snort version 3 with rule package updated.	

Troubleshooting

Se você encontrar problemas durante a atualização, considere estas etapas:

- Certifique-se de que suas versões de FTD sejam compatíveis com o Snort 3.

Para obter mais detalhes, consulte o [Guia de compatibilidade da Threat Defense do Cisco Secure Firewall](#)

- Colete os arquivos de solução de problemas no FDM navegando até a guia Dispositivo e clicando em Solicitar que o arquivo seja criado. Depois de coletado, abra um caso com o TAC e carregue o arquivo para o caso para obter mais assistência.

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

Informações Relacionadas

- [Adoção do Snort 3](#)
- [Documentos do Snort](#)
- [Guia de configuração do gerenciador de dispositivos do Cisco Secure Firewall, versão 7.2](#)

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.