# Atualização do Snort 2 para o Snort 3 via FMC

### Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Atualize a versão do Snort
Método 1
Método 2
Atualização das regras de intrusão
Verificar
Troubleshooting
Informações Relacionadas

### Introdução

Este documento descreve como atualizar as versões Snort 2 e Snort 3 no Firepower Manager Center (FMC).

#### Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense
- Firepower Management Center
- Snort

#### **Componentes Utilizados**

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

- FMC 7.0
- FTD 7.0

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) e do Cisco Defense Orchestrator (CDO); na versão 7.0 do Firepower Management Center (FMC).

O Snort 3.0 foi projetado para lidar com estes desafios:

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

### Configurar

Atualize a versão do Snort

Método 1

1. Faça login no Firepower Management Center.

2. Na guia Dispositivo, navegue até Dispositivos > Gerenciador de dispositivos.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devi	ces Objects	Integration
Summary Dashboard (setter dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Ge	eolocation	QoS	De De NJ e: VP	vice Management vice Upgrade N	QoS Platform Settings FlexConfig Certificates
<ul> <li>Unique Applications over Time</li> </ul>			- ×	Si Re Dy Tr	e To Site mote Access namic Access Policy publeshooting	

3. Selecione o dispositivo cuja versão do Snort você deseja alterar.

View By: All (2)	Group • Error (0) • W	• aming (0)	Offline (0)	Normal (2)	• De	eployment Pending (1)	• Upgr	ade (0)	
Collapse All									
Name	0					Model		Version	Chassis
□ ~ HA	(1)								
• •	HA-CALO-LAB High Availability								
	192.168.1.14(Prima 192.168.1.14 - Rout	ry, Active) led				FTDv for VMware		7.0.5	N/A
	2 192.168.1.15(Seco 192.168.1.15 - Rou	ndary, Standby) led				FTDv for VMware		7.0.5	N/A

4. Clique na guia Dispositivo e clique no botão Atualizar na seção Mecanismo de inspeção.

IA-CALO-LAB isco Firepower Threat Defense for VMware						
Summary High Availability Device 5	Routing Interfaces Inline Sets D	HCP				
				192.168	1.14 •	
General	/±7	System	0 G	Inspection Engine		
Name:	192.168.1.14	Model	Cisco Firepower Threat Defense for VMware	Inspection Engine:	Snort 2	
Transfer Packets:	Yes	Serial.	SAEMADW0934	NEW Upgrade to our new and improved Snort 3		
Mode:	Routed	Time:	2024-04-11 15:47:36	Snort 3 is the latest version of the most powerful, industry-standard inspection		
Compliance Mode:	None	Time Zone:	UTC (UTC+0:00)	improvements to performance and security efficacy, there	is a lot to be excited	
TLS Crypto Acceleration:	Disabled	Version:	7.0.5	about Learn more		
		Time Zone setting for Time based Rules.	UTC (UTC+0.00)	Because Short must be stopped so that the new version ca be momentary traffic loss.	in be started, there will	
				Note: If the device uses an Intrusion Policy that has custom will not be able to migrate those rules.	Intrusion Rule, Snort 3	
				Uppede		

5. Confirme sua seleção.



Método 2

1. Faça login no Firepower Management Center.

2. Na guia Dispositivo, navegue até Dispositivos > Gerenciador de dispositivos.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devi	ces Objects	Integration
Summary Dashboard (setter dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Ge	eolocation	QoS	De De NJ e: VP	vice Management vice Upgrade N	QoS Platform Settings FlexConfig Certificates
<ul> <li>Unique Applications over Time</li> </ul>			- ×	Si Re Dy Tr	e To Site mote Access namic Access Policy publeshooting	

3. Selecione o dispositivo cuja versão do Snort você deseja alterar.

View By:	Group	*				
All (2)	Error (0)     Warning (0)	<ul> <li>Offline (0)</li> </ul>	Normal (2)	Deployment Pending (1)	<ul> <li>Upgrade (0)</li> </ul>	
Collapse All						
Na	me			Model	Version	Chassis
	IA (1)					
• •	HA-CALO-LAB High Availability					
	192.168.1.14(Primary, Active) 192.168.1.14 - Routed			FTDv for VMware	7.0.5	N/A
	2 192.168.1.15(Secondary, Stand 192.168.1.15 - Routed	by)		FTDv for VMware	7.0.5	N/A

4. Clique no Selecionar Ação botão e selecione Atualizar para Snort 3.



Atualização das regras de intrusão

Além disso, você precisa converter suas regras do Snort 2 em regras do Snort 3.

1. Selecione no menu Objetos > Regras de intrusão.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
lescription, or l	Base Policy			Object M Intrusion	lanagemen Rules	t

2.Selecione no menu Snort 2 All Rules tab > Group Rules By > Local Rules.



3. Clique em Snort 3 All Rules guia e certifique-se de que All Rules está selecionado.

Snort 2 All Rules	Snort 3 All Rules
< Intrusion Policy	
67 items	Q Search Rule Group
All Rules	

4.No menu suspenso Task, selecione Convert and import.



5. Clique em OK na mensagem de advertência.

Convert and import
The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.
Cancel OK

#### Verificar

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



A conversão da regra foi bem-sucedida quando você recebeu esta mensagem:



Finalmente, você deve encontrar no Local Rules grupo a seção All Snort 2 Converted Global , que contém todas as suas regras Snort 2 para Snort 3 convertidas.



## Troubleshooting

Caso a migração falhe ou trave, reverta para o Snort 2 e tente novamente.

### Informações Relacionadas

- Como migrar do Snort 2 para o Snort 3
- Cisco Secure Atualização de Snort 3 Dispositivos (Vídeo Externo no YouTube)

#### 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.