

Roteador e Security Device Manager no exemplo da configuração de sistema da prevenção de intrusão do Cisco IOS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como usar a versão 2.5 de Roteador Cisco e Security Device Manager (SDM) a fim configurar o Intrusion Prevention System (IPS) do ^{® do} Cisco IOS em 12.4(15)T3 e em umas liberações mais atrasadas.

Os realces em SDM 2.5 relacionado a IO IPS são:

- Totalize o número compilado da assinatura indicado na lista de assinatura GUI
- Arquivos de assinatura SDM (formato de arquivo zip; por exemplo, sigv5-SDM-S307.zip) e da assinatura CLI pacotes (formato de arquivo de pacote; por exemplo, IOS-S313-CLI.pkg) pode ser transferido junto em uma operação
- Os pacotes transferidos da assinatura podem ser empurrados automaticamente para o roteador como uma opção

As tarefas envolvidas no processo de provisionamento inicial são:

1. Transfira e instale SDM 2.5.
2. Use a auto atualização SDM a fim transferir o pacote da assinatura IO IPS a um PC local.
3. Lance o assistente das políticas IPS a fim configurar IO IPS.
4. Verifique que a configuração e as assinaturas IO IPS estão carregadas corretamente

Cisco SDM é uma ferramenta de configuração com base na Web que simplifique o roteador e a configuração de segurança através dos assistentes espertos que ajudam clientes rapidamente e facilmente distribuem, configuram, e monitoram um roteador Cisco sem exigir o conhecimento do comando line interface(cli).

A versão 2.5 SDM pode ser transferida de Cisco.com em <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm> (clientes registrados somente). O Release Note pode ser encontrado em http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/soft

[ware/release/notes/SDMr25.html](http://www.cisco.com/ware/release/notes/SDMr25.html)

Nota: Cisco SDM exige uma definição da tela pelo menos de 1024 x de 768.

Nota: Cisco SDM exige o tamanho da memória heap das Javas ser nenhum menos do que 256MB a fim configurar IO IPS. A fim mudar o tamanho da memória heap das Javas, abra o painel de controle de Java, clique a aba das **Javas**, clique a **vista** situada sob os ajustes do Runtime do Java applet, e incorpore então **-Xmx256m** à coluna de parâmetro do tempo de execução de Java.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS IPS em 12.4(15)T3 e em liberações mais atrasadas
- Versão 2.5 de Roteador Cisco e Security Device Manager (SDM)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

Nota: Abra uma sessão do console ou do telnet ao roteador (com do “o monitor termo” sobre) a fim monitorar mensagens quando você usa o SDM para provision IO IPS.

1. Transfira SDM 2.5 do cisco.com em <http://www.cisco.com/cgi-bin/tablebuild.pl/sdm> ([clientes registrados somente](#)) e instale-o em um PC local.
2. Execute SDM 2.5 do PC local.
3. Quando a caixa de diálogo do início de uma sessão IO IPS aparece, incorpore o mesmos nome de usuário e senha que você usa para a autenticação SDM ao roteador.
4. Da interface do utilizador SDM, o clique **configura**, e clica então a **prevenção de intrusão**.
5. Clique a aba **IPS da edição**.
6. Se a notificação SDEE não é permitida no roteador, clique a **APROVAÇÃO** a fim permitir a notificação SDEE.
7. No arquivo de assinatura da transferência da área do cisco.com da aba IPS da edição, clique a **obtenção o arquivo o mais atrasado SDM e do pacote CLI** botão de rádio, e clique-a

então **consultam** a fim selecionar um diretório em seu PC local em que para salvar os arquivos baixados. Você pode escolher o diretório raiz TFTP ou de servidor FTP, que estará usado mais tarde quando você distribui o pacote da assinatura ao roteador.

8. Clique em **Download**.
9. Quando a caixa de diálogo do início de uma sessão CCO aparece, use seus nome e senha de usuário registrado CCO. O SDM conecta ao cisco.com e começa transferir ambos o arquivo SDM (por exemplo, sigv5-SDM-S307.zip) e o arquivo de pacote CLI (por exemplo, IOS-S313-CLI.pkg) ao diretório selecionado na etapa 7. Uma vez que ambos os arquivos são transferidos, o SDM alerta-o empurrar o pacote transferido da assinatura para o roteador.
10. Clique o **nenhum** desde que os IO IPS não foram configurados no roteador ainda.
11. Após o SDM transfere o pacote o mais atrasado da assinatura do IOS CLI, clicam a aba **IPS da criação** a fim criar a configuração inicial IO IPS.
12. Se você é alertado aplicar mudanças ao roteador, o clique **aplica mudanças**.
13. **Assistente da regra IPS do lançamento do clique.** Uma caixa de diálogo parece informá-lo que o SDM precisa de estabelecer uma assinatura SDEE ao roteador para recuperar alertas.
14. Clique em **OK**. A autenticação exigiu a caixa de diálogo aparece.
15. Incorpore o nome de usuário e a senha que você se usou para o SDM para autenticar ao roteador, e clique a **APROVAÇÃO**. A caixa de diálogo do assistente das políticas IPS aparece.
16. Clique em Next.
17. No indicador das interfaces selecionada, escolha a relação e o sentido a que esse os IO IPS serão aplicados, e clique-os então **ao lado de** continuam.
18. Na área do arquivo de assinatura do indicador do arquivo de assinatura e da chave pública, clique a **especificação o arquivo de assinatura que você quer se usar com o** botão de rádio **IO IPS**, e clique então o botão do **arquivo de assinatura (...)** a fim especificar o lugar do arquivo de pacote da assinatura, que será o diretório especificado na etapa 7.
19. Clique o **arquivo de assinatura da especificação usando o** botão de rádio **URL**, e escolha um protocolo da lista de drop-down do protocolo. **Nota:** Este exemplo usa o TFTP a fim transferir o pacote da assinatura ao roteador.
20. Incorpore a URL para o arquivo de assinatura, e clique a **APROVAÇÃO**.
21. Na área de chave pública configurar do indicador do arquivo de assinatura e da chave pública, incorpore **realm-cisco.pub** ao campo de nome, e então copie esta chave pública e **cole-a no campo chave**. 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A

02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001 **Nota:** Esta chave pública pode ser transferência do cisco.com em: <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup> (clientes registrados somente).

22. Clique em Avançar para continuar.
23. No indicador do lugar e da categoria da configuração, clique o botão do **lugar da configuração (...)** a fim especificar um lugar onde a definição e os arquivos de configuração das assinaturas sejam armazenados. A caixa de diálogo do **lugar da configuração adicionar** aparece.
24. Na caixa de diálogo do lugar da configuração adicionar, clique a **especificação o lugar da configuração neste** botão de rádio do **roteador**, e clique então o botão do **nome de diretório (...)** a fim encontrar o arquivo de configuração. A caixa de diálogo do dobrador da escolha aparece a fim permitir que você selecione um diretório existente ou crie um diretório novo no flash de roteador para armazenar a definição e os arquivos de configuração da assinatura.
25. Clique o **dobrador novo** situado na parte superior da caixa de diálogo se você quer criar um diretório novo.
26. Uma vez que você seleciona o diretório, clique a **APROVAÇÃO** a fim aplicar mudanças, e clique então a **APROVAÇÃO** a fim fechar a caixa de diálogo do lugar da configuração adicionar.
27. Na caixa de diálogo do assistente das políticas IPS, selecione a categoria da assinatura de acordo com a quantidade de memória instalada no roteador. Há duas categorias que da assinatura você pode escolher no SDM: Básico e avançado. Se o roteador tem 128MB DRAM instalado, Cisco recomenda que você escolha a categoria de básica a fim evitar falhas de alocação de memória. Se o roteador tem 256MB ou mais DRAM instalado, você pode escolher uma ou outra categoria.
28. Uma vez que você seleciona uma categoria para se usar, para clicar **em seguida** a fim continuar à página de sumário. A página de sumário fornece uma breve descrição sobre a configuração inicial das tarefas IO IPS.
29. Clique o **revestimento na** página de sumário a fim entregar as configurações e o pacote da assinatura ao roteador. Se os comandos option da estreia são permitidos nos ajustes das preferências no SDM, o SDM indica a configuração do fornecimento à caixa de diálogo do roteador que mostra um sumário dos comandos CLI que o SDM entrega ao roteador.
30. O clique **entrega** a fim continuar. A caixa do diálogo de status da entrega dos comandos parece mostrar o estado da entrega dos comandos.
31. Quando os comandos são entregados ao roteador, clique a **APROVAÇÃO** a fim continuar. A caixa de diálogo do Status de Configuração IO IPS mostra que as assinaturas estão sendo carregadas no roteador.
32. Quando as assinaturas são carregadas, o SDM indica a aba **IPS da edição** com a configuração atual. Verifique que relação e em que sentido os IO IPS são permitidos a fim verificar a configuração. O console de roteador mostra que as assinaturas estiveram carregadas.
33. Use o **comando count das assinaturas da mostra IP IP** a fim verificar que as assinaturas estão carregadas corretamente.

```
router#show ip ips signatures count Cisco SDF release version S313.0 Trend SDF release version V0.0 | snip | Total Signatures: 2158 Total Enabled Signatures: 829 Total Retired Signatures: 1572 Total Compiled Signatures: 580 Total Signatures with invalid parameters: 6 Total Obsoleted Signatures: 11
```

 O abastecimento inicial de IO IPS que usam SDM 2.5 está completo.
34. Verifique os números da assinatura com o SDM segundo as indicações desta imagem.

Informações Relacionadas

- [Cisco IOS IPS no cisco.com](#)
- [Pacote da assinatura IPS do Cisco IOS](#)
- [Arquivos de assinatura IPS do Cisco IOS para o SDM](#)
- [Obtenção começado com Cisco IOS IPS com formato da assinatura 5.x](#)
- [Manual de configuração IPS do Cisco IOS](#)
- [Visualizador de eventos do Cisco IDS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)