Sistema da prevenção de intrusão com exemplo de configuração das assinaturas do formato 5.x

Índice

Introdução

Este documento descreve como configurar assinaturas do formato 5.x no ® IPS do Cisco IOS e é organizado em duas seções:

- Etapas de configuração de I. Getting Começo da seção — Esta seção fornece as etapas necessárias usar o comando line interface(cli) do Cisco IOS a fim obter começada com as assinaturas do formato IO IPS 5.x. Esta seção descreve estas etapas:Etapa 1. Transfira os arquivos IO IPS.Etapa 2. Crie um diretório de configuração IO IPS no flash.Etapa 3. Configurar uma chave de criptografia IO IPS.Etapa 4. Permita IO IPS.Etapa 5. Carregue o pacote da assinatura IO IPS ao roteador.Cada etapa e comandos específicos são descritos em detalhe, assim como comandos adicionais e referências. Um exemplo de configuração é indicado abaixo de cada comando.
- Opções de configuração avançadas da seção II. — Esta seção fornece instruções e exemplos em opções avançadas para o ajustamento da assinatura. Contém estas opções:Aposente-se ou assinaturas de UnretirePermita ou desabilite assinaturasMude ações de assinatura

Pré-requisitos

Requisitos

Assegure-se de que você tenha os componentes apropriados (como descrito nos componentes usados) antes que você termine as etapas neste documento.

Componentes Utilizados

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

- Um roteador dos Serviços integrados de Cisco (87x, 18xx, 28xx, ou 38xx)
- 128MB ou mais DRAM e pelo menos memória flash livre 2MB
- Console ou conectividade telnet ao roteador
- Cisco IOS Release 12.4(15)T3 ou Mais Recente
- Um nome e uma senha válidos de usuário de login CCO (cisco.com)
- Um contrato de serviço atual do ips Cisco para serviços licenciados da atualização de assinatura

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.

Secione etapas de configuração de I. Getting Começo

Etapa 1. Arquivos da transferência IO IPS

A primeira etapa é transferir arquivos de pacote da assinatura IO IPS e a chave de criptografia pública do cisco.com.

Transfira os arquivos de assinatura exigidos do cisco.com a seu PC:

- Lugar: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (clientes registrados somente)
- Arquivos a transferir:IOS-Sxxx-CLI.pkg (registeredcustomers somente) — Este é o pacote o mais atrasado da assinatura.realm-cisco.pub.key.txt (clientes registrados somente) — Esta é a chave de criptografia pública usada por IO IPS.

Etapa 2. Crie um diretório de configuração IO IPS no flash

O segundo passo é criar um diretório no flash do seu roteador onde você armazena os arquivos de assinatura e as configurações exigidos. Alternativamente, você pode usar uma movimentação do flash de Cisco USB conectada ao porta usb do roteador para armazenar os arquivos de assinatura e as configurações. A movimentação do flash USB deve permanecer conectada ao porta usb do roteador se é usada como o lugar do diretório de configuração IO IPS. OS IO IPS igualmente apoiam todo o sistema de arquivo IOS como seu local de configuração com acesso de

gravação apropriado.

A fim criar um diretório, incorpore este comando na alerta de roteador: *nome* **<directory do mkdir >**

Por exemplo:

```
router#mkdir ips Create directory filename [ips]? Created dir flash:ips
```

Comandos adicionais e referências

A fim verificar os índices do flash, incorpore este comando na alerta de roteador: **flash da mostra:**

Por exemplo:

```
router#dir flash: Directory of flash:/ 5 -rw- 51054864 Feb 8 2008 15:46:14 -08:00 c2800nm-
advipservicesk9-mz.124-15.T3.bin 6 drw- 0 Feb 14 2008 11:36:36 -08:00 ips 64016384 bytes total
(12693504 bytes free)
```

A fim rebatizar o nome de diretório, use este comando: **rebatize o** *nome* **<current > o** *nome do* **<new >**

Por exemplo:

```
router#rename ips ips_new Destination filename [ips_new]?
```

Etapa 3. Configurar uma chave de criptografia IO IPS

A terceira etapa é configurar a chave de criptografia usada por IO IPS. Esta chave é ficada situada no arquivo de realm-cisco.pub.key.txt que foi transferido em etapa 1.

A chave de criptografia é usada para verificar a assinatura digital para o arquivo de assinatura mestre (sigdef-default.xml) cujos os índices são assinados por uma chave privada de Cisco para garantir suas autenticidade e integridade em cada liberação.

1. Abra o arquivo de texto, e copie os índices do arquivo.
2. Use o **comando configure terminal** a fim inscrever o roteador configuram o modo.
3. Cole o índice do arquivo de texto na alerta do `<hostname>(config)#`.
4. Retire o modo de configuração do roteador.
5. Inscreva o **comando show run na** alerta de roteador a fim confirmar que a chave de criptografia está configurada. Você deve ver esta saída na configuração:
```
crypto key pubkey-
chain rsa
named-key realm-cisco.pub signature
key-string
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
Quit
```
6. Utilize este comando para salvar a configuração:**a cópia executar-configura partida-configura**

Comandos adicionais e referências

Se a chave é configurada incorretamente, você deve remover a chave de criptografia primeiramente e então reconfigurá-la:

1. A fim remover a chave, incorpore estes comandos à ordem alistada abaixo:`router#configure terminal router(config)#no crypto key pubkey-chain rsa router(config-pubkey-chain)#no named-key realm-cisco.pub signature router(config-pubkey-chain)#exit router(config)#exit`
2. Use o **comando show run** a fim verificar que a chave está removida da configuração.
3. Termine o procedimento em etapa 3 a fim reconfigurar a chave.

Etapa 4. Permita IO IPS

A quarta etapa é configurar IO IPS. Termine este procedimento a fim configurar IO IPS:

1. Use o *nome do* **<rule do nome IP IP > <** comando *ACL opcional* **>** a fim criar um nome da regra. (Isto será usado em uma relação para permitir o IPS.)Por exemplo:`router#configure terminal router(config)#ip ips name iosips` Você pode especificar um Access Control List prolongado ou padrão opcional (ACL) a fim filtrar o tráfego que será feito a varredura por este nome da regra. Todo o tráfego que é permitido pelo ACL é sujeito à inspeção pelo IPS. Trafique que é negado pelo ACL não é inspecionado pelo IPS.`router(config)#ip ips name ips list ? <1-199> Numbered access list WORD Named access list`
2. Use o **flash do lugar da configuração IP IP:** *nome* **>** comando **<directory** a fim configurar o local de armazenamento da assinatura IPS. (Este é o diretório *IP* criado em etapa 2.)Por exemplo:`router(config)#ip ips config location flash:ips`
3. Use o **IP IP notificam o** comando do **sdee** a fim permitir a notificação de evento IPS SDEE.Por exemplo:`router(config)#ip ips notify sdee` A fim usar SDEE, o Server do HTTP deve ser permitido (com o **comando ip http server**). Se o Server do HTTP não é permitido, o roteador não pode responder aos clientes SDEE porque não pode ver os pedidos. A notificação SDEE é desabilitada à revelia e deve explicitamente ser permitida.OS IO IPS igualmente apoiam o uso do Syslog a fim enviar a notificação de evento. SDEE e o Syslog podem ser usados independentemente ou permitido ao mesmo tempo a fim enviar a notificação de evento IO IPS. A notificação de SYSLOG é permitida à revelia. Se o console de registro é permitido, você verá mensagens do syslog IPS. A fim permitir o Syslog, use este comando:`router(config)#ip ips notify log`
4. Configurar IO IPS para usar uma das categorias predefinidas da assinatura.OS IO IPS com as assinaturas do formato de Cisco 5.x operam-se com categorias da assinatura (apenas como dispositivos do ips Cisco). Todas as assinaturas são agrupadas em categorias, e as categorias são hierárquicas. Isto ajuda a classificar assinaturas para o agrupamento e o ajustamento fáceis.**aviso:** *Toda a* categoria da assinatura contém todas as assinaturas em uma liberação da assinatura. Desde que os IO IPS não podem compilar e para usar todas as assinaturas contidas em uma assinatura libere ao mesmo tempo, *não faz o unretire toda a categoria*; se não, o roteador será executado fora da memória.**Nota:** Quando você configura IO IPS, você deve primeiramente aposentar-se todas as assinaturas em *toda a* categoria, e então o unretire selecionou categorias da assinatura.**Nota:** A ordem em que as categorias da assinatura são configuradas no roteador é igualmente importante. OS IO IPS processam os comandos da categoria na ordem alistada na configuração. Algumas assinaturas pertencem às categorias múltiplas. Se as categorias múltiplas são configuradas e uma assinatura pertence a mais de uma delas, as propriedades da assinatura (por exemplo, aposentado, unretired, ações, etc.) na última categoria configurada estão usadas por IO IPS.Neste exemplo, todas as assinaturas em “toda a” categoria são aposentadas, e então a *categoria*

de básica IO IPS unretired.`router(config)#ip ips signature-category router(config-ips-category)#category all router(config-ips-category-action)#retired true router(config-ips-category-action)#exit router(config-ips-category)#category ios_ips basic router(config-ips-category-action)#retired false router(config-ips-category-action)#exit router(config-ips-category)#exit Do you want to accept these changes? [confirm]y router(config)#`

5. Use estes comandos a fim permitir a regra IPS na interface desejada, e especifique o sentido em que a regra será aplicada:**conecte o** *nome do* **<interface >***nome do* **<rule IP IP > [***em | para fora***]**Por exemplo:`router(config)#interface GigabitEthernet 0/1 router(config-if)#ip ips iosips in router(config-if)#exit router(config)#exit router#` No argumento significa que somente o tráfego que entra na relação está inspecionado pelo IPS. O argumento da *saída* significa que somente a saída do tráfego da relação está inspecionada pelo IPS.A fim permitir o IPS de inspecionar ambos em e para fora o tráfego da relação, dê entrada com separadamente o nome da regra IPS para *dentro* e *para fora na* mesma relação:`router(config)#interface GigabitEthernet 0/1 router(config-if)#ip ips iosips in router(config-if)#ip ips iosips out router(config-if)#exit router(config)#exit router#`

Etapa 5. Carregue o pacote da assinatura IO IPS ao roteador

A última etapa é carregar ao roteador que o pacote da assinatura transferiu em etapa 1.

Nota: A maioria de forma comum carregar o pacote da assinatura ao roteador é usar o FTP ou o TFTP. Este procedimento usa o FTP. Refira por favor a seção dos *comandos adicionais e de referências n*este procedimento para que um método alternativo carregue o pacote da assinatura IO IPS. Se você usa uma sessão de Telnet, use o **comando terminal monitor** a fim ver as saídas do console.

A fim carregar o pacote da assinatura ao roteador, termine estas etapas:

1. Use este comando a fim copiar o pacote transferido da assinatura do servidor FTP ao roteador:**copie o <ftp_user de ftp://***: idconf de password@Server_IP_address* **>/<signature_package>Nota:** Recorde por favor usar o parâmetro do *idconf na* extremidade do **comando copy**.**Nota:** Por exemplo:`router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 7608873/4096 bytes]` A compilação da assinatura começa imediatamente depois que o pacote da assinatura é carregado ao roteador. Você pode ver que entra o roteador com nível de registro 6 ou acima do permitido.
```
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED:
16:44:47 PST Feb 14 2008
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
                      packets for this engine will be scanned
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
                      packets for this engine will be scanned
|
output snipped
|
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures -
                      12 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms -
                      packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures -
                      13 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms -
```

```
                    packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

2. Use o **comando count da assinatura da mostra IP IP** a fim verificar que o pacote da assinatura está compilado corretamente.Por exemplo:`router#`**`show ip ips signature count`**
```
Cisco SDF release version S310.0  signature package release version Trend SDF release
version V0.0 Signature Micro-Engine: multi-string: Total Signatures 8 multi-string enabled
signatures: 8 multi-string retired signatures: 8 | outpt snipped | Signature Micro-Engine:
service-msrpc: Total Signatures 25 service-msrpc enabled signatures: 25 service-msrpc
retired signatures: 18 service-msrpc compiled signatures: 1 service-msrpc inactive
signatures - invalid params: 6 Total Signatures: 2136 Total Enabled Signatures: 807 Total
Retired Signatures: 1779 Total Compiled Signatures: 351  total compiled signatures for the
IOS IPS Basic category Total Signatures with invalid parameters: 6 Total Obsoleted
Signatures: 11 router#
```

Comandos adicionais e referências

A chave de criptografia pública é inválida se você recebe um Mensagem de Erro na altura da compilação da assinatura similar a este Mensagem de Erro:

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)
```

Refira etapa 3 para mais informação.

Se você não tem o acesso a um FTP ou a um servidor TFTP, você pode usar uma movimentação do flash USB a fim carregar o pacote da assinatura ao roteador. Primeiramente, copie o pacote da assinatura na movimentação USB, conecte a movimentação USB a um dos porta usb no roteador, e use então o **comando copy** com o parâmetro do *idconf* a fim copiar o pacote da assinatura ao roteador.

Por exemplo:

```
router#copy usbflash1:IOS-S310-CLI.pkg idconf
```

Há seis arquivos no diretório configurado do armazenamento IO IPS. Estes arquivos usam este formato do nome: <router-nome >-sigdef-xxx.xml ou < nome de roteador *>-seap-xxx.xml*.

```
router#dir ips Directory of flash:/ips/ 7 -rw- 203419 Feb 14 2008 16:45:24 -08:00 router-sigdef-
default.xml 8 -rw- 271 Feb 14 2008 16:43:36 -08:00 router-sigdef-delta.xml 9 -rw- 6159 Feb 14
2008 16:44:24 -08:00 router-sigdef-typedef.xml 10 -rw- 22873 Feb 14 2008 16:44:26 -08:00 router-
sigdef-category.xml 11 -rw- 257 Feb 14 2008 16:43:36 -08:00 router-seap-delta.xml 12 -rw- 491
Feb 14 2008 16:43:36 -08:00 router-seap-typedef.xml 64016384 bytes total (12693504 bytes free)
router#
```

Estes arquivos são armazenados em formato comprimido e não são diretamente editáveis ou visualizável. Os índices de cada arquivo são descritos abaixo:

- *router-sigdef-default.xml contém* todas as definições da assinatura do padrão de fábrica.
- *router-sigdef-delta.xml contém as* definições da assinatura que foram mudadas do padrão.
- *router-sigdef-typedef.xml contém* todas as definições de parâmetro da assinatura.
- *router-sigdef-category.xml contém a* informação da categoria da assinatura, tal como ios_ips da categoria básicos e avançados.
- *router-seap-delta.xml contém as* mudanças feitas aos parâmetros do padrão SEAP.
- *router-seap-typedef.xml contém* todas as definições de parâmetro SEAP.

Opções de configuração avançadas da seção II.

Esta seção fornece instruções e exemplos em opções avançadas IO IPS para o ajustamento da assinatura.

Assinaturas aposente-se ou de Unretire

Para aposentar-se ou unretire meios de uma assinatura selecionar ou deselect as assinaturas que são usadas por IO IPS a fim fazer a varredura do tráfego.

- **Aposentar-se uma** assinatura significa que os IO IPS não compilarão essa assinatura na memória para fazer a varredura.
- **Unretiring uma** assinatura instrui IO IPS para compilar a assinatura na memória e para usar a assinatura para fazer a varredura do tráfego.

Você pode usar o comando line interface(cli) IO a fim assinaturas individuais aposentar-se ou de unretire ou um grupo de assinaturas que pertencem a uma categoria da assinatura. Quando você se aposenta ou unretire um o grupo de assinaturas, todas as assinaturas nessa categoria estão aposentadas ou unretired.

Nota: Algumas assinaturas unretired (unretired como a assinatura individual ou dentro de uma categoria unretired) não podem compilar devido à memória insuficiente ou aos parâmetros inválidos ou se a assinatura obsoleted.

Este exemplo mostra como aposentar-se assinaturas individuais. Por exemplo, assinatura 6130 com subsig ID do 10:

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status router(config-sigdef-sig-status)#retired true router(config-
sigdef-sig-status)#exit router(config-sigdef-sig)#exit router(config-sigdef)#exit Do you want to
accept these changes? [confirm]y router(config)#
```

Este exemplo mostra como ao unretire todas as assinaturas que pertencem à categoria de básica IO IPS:

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false router(config-ips-category-action)#exit
router(config-ips-category)#exit Do you want to accept these changes? [confirm]y
```

Nota: Quando as assinaturas nas categorias diferentes de IO IPS básicos e de IO IPS avançados unretired como uma categoria, a compilação de alguns assinaturas ou motores poderia falhar porque determinadas assinaturas naquelas categorias não são apoiadas por IO IPS (veja o exemplo abaixo). Todo o outro assinaturas (unretired) com sucesso compiladas é usado por IO IPS para fazer a varredura do tráfego.

```
Router(config)#ip ips signature-category router(config-ips-category)#category os router(config-
ips-category-action)#retired false router(config-ips-category-action)#exit router(config-ips-
category)#exit Do you want to accept these changes? [confirm]y *Feb 14 18:10:46 PST: Applying
Category configuration to signatures ... *Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDS_STARTED:
08:10:49 PST Feb 18 2008 *Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8
signatures - 1 of 13 engines *Feb 14 18:10:49 PST: %IPS-6-ENGINE_READY: multi-string - build
time 136 ms - packets for this engine will be scanned *Feb 14 18:10:49 PST: %IPS-6-
ENGINE_BUILDING: service-http - 622 signatures - 2 of 13 engines *Feb 14 18:10:50 PST: %IPS-4-
META_ENGINE_UNSUPPORTED: service-http 5903:1 - this signature is a component of the unsupported
META engine *Feb 14 18:24:42 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5754:0 -
compilation of regular expression failed *Feb 14 18:24:49 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE:
service-http 5729:1 - compilation of regular expression failed
```

Permita ou desabilite assinaturas

Para permitir ou desabilitar uma assinatura são reforçar ou negligenciar as ações associadas com as assinaturas por IO IPS quando o pacote ou o fluxo de pacote de informação combinam as

assinaturas.

Nota: Permita e o desabilitação não seleciona e deselect assinaturas para ser usado por IO IPS.

- Para **permitir uma** assinatura significa que quando provocada por um pacote de harmonização (ou pelo fluxo de pacote de informação), a assinatura toma a ação apropriada associada com ela. Contudo, as assinaturas somente unretired E com sucesso compiladas tomarão a ação quando são permitidas. Ou seja se uma assinatura é aposentada, mesmo que seja permitido, não será compilada (porque é aposentada) e não tomará a ação associada com ela.
- Para **desabilitar uma** assinatura significa que quando provocada por um pacote de harmonização (ou pelo fluxo de pacote de informação), a assinatura não toma a ação apropriada associada com ela. Ou seja quando uma assinatura é desabilitada, mesmo que unretired e seja compilado com sucesso, não tomará a ação associada com ela.

Você pode usar o comando line interface(cli) IO a fim permitir ou desabilitar assinaturas individuais ou um grupo de assinaturas baseadas em categorias da assinatura. Este exemplo mostra como desabilitar a assinatura 6130 com subsig ID do 10.

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status router(config-sigdef-sig-status)#enabled false router(config-
sigdef-sig-status)#exit router(config-sigdef-sig)#exit router(config-sigdef)#exit Do you want to
accept these changes? [confirm]y router(config)#
```

Este exemplo mostra como permitir todas as assinaturas que pertencem à categoria de básica IO IPS.

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#enabled true router(config-ips-category-action)#exit
router(config-ips-category)#exit Do you want to accept these changes? [confirm]y router(config)#
```

Mude ações de assinatura

Você pode usar o comando line interface(cli) IO a fim mudar ações de assinatura para uma assinatura ou um grupo de assinaturas baseadas em categorias da assinatura. Este exemplo mostra como mudar ações de assinatura alertar, deixar cair, e restauração para a assinatura 6130 com subsig ID do 10.

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#engine router(config-sigdef-sig-engine)#event-action produce-alert
router(config-sigdef-sig-engine)#event-action deny-packet-inline router(config-sigdef-sig-
engine)#event-action reset-tcp-connection router(config-sigdef-sig-engine)#exit router(config-
sigdef-sig)#exit router(config-sigdef)#exit Do you want to accept these changes? [confirm]y
router(config)#
```

Este exemplo mostra como mudar ações do evento para todas as assinaturas que pertencem à categoria de básica da assinatura IO IPS.

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#event-action produce-alert router(config-ips-category-
action)#event-action deny-packet-inline router(config-ips-category-action)#event-action reset-
tcp-connection router(config-ips-category-action)#exit router(config-ips-category)#exit Do you
want to accept these changes? [confirm]y router(config)#
```

Informações Relacionadas

- Página do Produtos & dos serviços do Cisco IOS Intrusion Prevention System (IPS)
- Cisco IOS IPS - Download do software das assinaturas da versão 5
- Realces IPS do apoio e da usabilidade do formato da assinatura 5.x
- Download do software do gerenciador do dispositivo de segurança da Cisco
- Como usar o CCP para configurar IO IPS
- Transferência de software criptográfico do visualizador de eventos 3DES do Sistema de Detecção de Intrusão da Cisco
- Suporte Técnico e Documentação - Cisco Systems