Roteador e Security Device Manager (SDM) e IOS Cisco CLI no exemplo de configuração do Cisco IOS Intrusion Prevention System (IPS)

Índice

Introdução

Em Roteador Cisco e Security Device Manager (SDM) 2.2, a configuração IPS do ® do Cisco IOS é integrada dentro do aplicativo SDM. Você é exigido já não lançar uma janela separada a fim configurar o Cisco IOS IPS.

Em Cisco SDM 2.2, um wizard de configuração novo IPS guia-o com as etapas necessárias permite o Cisco IOS IPS no roteador. Além, você pode ainda usar as opções de configuração avançadas permitir, desabilitar, e ajustar o Cisco IOS IPS com Cisco SDM 2.2.

Cisco recomenda que você executa o Cisco IOS IPS com os arquivos de definição pretuned da assinatura (SDFs): attack-drop.sdf, 128MB.sdf, e 256MB.sdf. Estes arquivos são criados para o Roteadores com as quantidades de memória diferentes. Os arquivos são empacotados com Cisco SDM, que recomenda SDFs quando você permite primeiramente o Cisco IOS IPS em um roteador. Estes arquivos podem igualmente ser transferidos de http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers somente).

O processo para permitir o padrão SDFs é detalhado dentro permite o Cisco IOS IPS com um padrão de fábrica SDF. Quando o padrão SDFs não é suficiente ou você quer adicionar assinaturas novas, você pode usar o procedimento descrito dentro adiciona assinaturas adicionais após ter permitido o padrão SDF.

Pré-requisitos

Requisitos

A versão 1.4.2 ou mais recente do ambiente de tempo de execução de java (JRE) é exigida para usar Cisco SDM 2.2. Um arquivo de assinatura Cisco-recomendado e ajustado (baseado no DRAM) é empacotado com Cisco SDM (carregado na memória de flash de roteador com Cisco SDM).

Componentes Utilizados

A informação neste documento é baseada em Roteador Cisco e Security Device Manager (SDM) 2.2.

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

Permita o Cisco IOS IPS com um padrão de fábrica SDF

Procedimento CLI

Termine este procedimento a fim usar o CLI para configurar um Cisco 1800 Series Router com Cisco IOS IPS para carregar 128MB.sdf no flash de roteador.

1. Configurar o roteador para permitir a notificação de evento da troca do evento do dispositivo de segurança (SDEE).`yourname#`**`conf t`**
2. Inscreva os comandos configuration (um pela linha), e pressione então Cntl+Z para terminar.`yourname(config)#`**`ip ips notify sdee`**
3. Crie um nome da regra IPS que seja usado para associar às relações.`yourname(config)#`**`ip ips name myips`**
4. Configurar um comando location IPS especificar de que arquivo o sistema IPS do Cisco IOS lerá assinaturas.Este exemplo usa o arquivo no flash: 128MB.sdf. A parcela do lugar URL deste comando pode ser toda a URL válida que usar o flash, o disco, ou os protocolos através do FTP, do HTTP, do HTTPS, do RTP, do SCP, e do TFTP a fim apontar aos arquivos.`yourname(config)#`**`ip ips sdf location flash:128MB.sdf`** **Nota:** Você deve permitir o **comando terminal monitor** se você configura o roteador através de uma sessão de Telnet ou você não verá as mensagens SDEE quando o Engine de assinatura está construindo.
5. Permita o IPS na relação onde você quer permitir o Cisco IOS IPS de fazer a varredura do tráfego. Neste caso, nós permitimos em ambos sentidos nos FastEthernet 0 da relação.`yourname(config)#`**`interface fastEthernet 0`** `yourname(config-if)#`**`ip ips myips in`** `*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl *Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from flash:128MB.sdf *Oct 26`

```
00:32:30.921: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines *Oct 26
00:32:30.921: %IPS-6-ENGINE_READY: OTHER - 0 ms - packets for this engines will be scanned
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new
signature definitions for this engine *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
STRING.ICMP - 1 signatures - 3 of 15 engines *Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
STRING.ICMP - 20 ms - packets for this engine will be scanned *Oct 26 00:32:30.945: %IPS-6-
ENGINE_BUILDING: STRING.UDP - 17 signatures - 4 of15 engines *Oct 26 00:32:31.393: %IPS-6-
ENGINE_READY: STRING.UDP - 448 ms - packets for this engine will be scanned *Oct 26
00:32:31.393: %IPS-6-ENGINE_BUILDING: STRING.TCP - 58 signatures - 5 of 15 engines *Oct 26
00:32:33.641: %IPS-6-ENGINE_READY: STRING.TCP - 2248 ms - packets for this engine will be
scanned *Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15
engines *Oct 26 00:32:33.657: %IPS-6-ENGINE_READY: SERVICE.FTP - 16 ms - packets for this
engine will be scanned *Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2
signatures - 7 of 15 engines *Oct 26 00:32:33.685: %IPS-6-ENGINE_READY: SERVICE.SMTP - 28
ms - packets for this engine will be scanned *Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
SERVICE.RPC - 29 signatures - 8 f 15 engines *Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
SERVICE.RPC - 92 ms - packets for this engine will be scanned *Oct 26 00:32:33.781: %IPS-6-
ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines *Oct 26 00:32:33.801: %IPS-
6-ENGINE_READY: SERVICE.DNS - 20 ms - packets for this engine will be scanned *Oct 26
00:32:33.801: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures - 10 of 15 engines *Oct
26 00:32:44.505: %IPS-6-ENGINE_READY: SERVICE.HTTP - 10704 ms - packets for this engine
will be scanned *Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
11 of 15 engines *Oct 26 00:32:44.513: %IPS-6-ENGINE_READY: ATOMIC.TCP - 4 ms - packets for
this engine will be scanned *Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9
signatures - 12 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.UDP - 4 ms
- packets for this engine will be scanned *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
ATOMIC.ICMP - 0 signatures - 13 of 15 engines *Oct 26 00:32:44.517: %IPS-6-
ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15
engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.IPOPTIONS - 0 ms - packets for
this engine will be scanned *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5
signatures - 15 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.L3.IP - 0
ms - packets for this engine will be scanned yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```

A primeira vez que uma regra IPS é aplicada a uma relação, os começos IPS do Cisco IOS construíram assinaturas do arquivo especificado pelo comando dos lugar SDF. As mensagens SDEE são registradas ao console e enviadas ao servidor de SYSLOG se configuradas. As mensagens SDEE com o <number> dos motores do <number> indicam o processo de construção do Engine de assinatura. Finalmente, quando os dois números são os mesmos, todos os motores são construídos.**Nota:** A remontagem virtual IP é uma característica da relação essa (quando girado sobre) remonta automaticamente os pacotes fragmentados que entram o roteador através dessa relação. Cisco recomenda que você permite o virtual-conjunto IP em todas as relações onde o tráfego entra o roteador. No exemplo acima, além de girar sobre “o virtual-conjunto IP” nos FastEthernet 0 da relação, nós configurar-lo na interface interna VLAN1 também.`yourname(config)#int vlan 1 yourname(config-if)#ip virtual-reassembly`

Procedimento SDM 2.2

Termine este procedimento a fim usar Cisco SDM 2.2 para configurar um Cisco 1800 Series Router com Cisco IOS IPS.

1. No aplicativo SDM, o clique **configura**, e clica então a **prevenção de intrusão**.
2. Clique a aba **IPS da criação**, e clique então o **assistente da regra IPS do lançamento**.Cisco SDM exige a notificação de evento IPS através de SDEE a fim configurar a característica IPS do Cisco IOS. À revelia, a notificação SDEE não é permitida. Cisco SDM alerta-o permitir a notificação de evento IPS através de SDEE segundo as indicações desta imagem:

3. Clique em **OK**.A boa vinda ao wizard do assistente das políticas IPS da caixa de diálogo do assistente das políticas IPS aparece.
4. Clique em Next.O indicador seleto das relações aparece.
5. Escolha as relações para que você quer permitir o IPS, e clique a caixa de seleção **de entrada** ou **de partida** a fim indicar o sentido dessa relação.**Nota:** Cisco recomenda que você permite de entrada e direções externas quando você permite o IPS em uma relação.
6. Clique em Next.O indicador dos lugar SDF aparece.
7. O clique **adiciona** a fim configurar um lugar SDF.Adicionar uma caixa de diálogo do lugar da assinatura aparece.
8. Clique a **especificação SDF no** botão de rádio **instantâneo**, e escolha 256MB.sdf do **nome de arquivo na** lista de drop-down **instantânea**.
9. Clique a caixa de seleção do **autosave**, e clique a **APROVAÇÃO**.**Nota:** A opção do autosave salvar automaticamente o arquivo de assinatura quando há uma mudança da assinatura.O indicador dos lugar SDF indica o lugar novo SDF.**Nota:** Você pode adicionar lugar adicionais da assinatura a fim designar um backup.
10. Clique a caixa de verificação **incorporado das assinaturas do uso (como o backup)**.**Nota:** Cisco recomenda que você não usa a opção incorporado da assinatura a menos que você especificar uns ou vários lugar.
11. Clique **em seguida** a fim continuar.A janela de sumário aparece.
12. Clique em Finish.A caixa do diálogo de status da entrega dos comandos indica o estado enquanto o motor IPS compila todas as assinaturas.
13. Uma vez o processo está completo, **APROVAÇÃO do** clique.A caixa do diálogo de status da compilação da assinatura indica a informação da compilação da assinatura.Esta informação mostra que motores foram compilados e o número de assinaturas nesse motor. Para os motores que indicam *saltado na* coluna de status, não há nenhuma assinatura carregada para esse motor.
14. Clique **próximo** a fim fechar a caixa do diálogo de status da compilação da assinatura.
15. A fim verificar que assinaturas são carregadas atualmente no roteador, o clique **configura**, e clica então a **prevenção de intrusão**.
16. Clique a aba **IPS da edição**, e clique então **assinaturas**.A lista de assinatura IPS aparece no indicador das assinaturas.

Adicione assinaturas adicionais após ter permitido o padrão SDF

Procedimento CLI

Não há nenhum comando CLI disponível para criar assinaturas ou ler a informação de assinatura do arquivo distribuído IOS-Sxxx.zip. Cisco recomenda que você usa o SDM ou o centro de gerenciamento para sensores IPS para controlar as assinaturas em sistemas IPS do Cisco IOS.

Para os clientes que já têm um arquivo de assinatura pronto e o querem fundir este arquivo com o SDF que é executado em um sistema IPS do Cisco IOS, você pode usar este comando:

```
yourname#show running-config | include ip ips sdf ip ips sdf location flash:128MB.sdf yourname#
```

O arquivo de assinatura definido pelo comando location da assinatura é onde o roteador carrega arquivos de assinaturas quando recarrega ou quando o roteador IO IPS está reconfigurado. Para que o processo de fusão seja bem sucedido, o arquivo definido pelo comando location do arquivo de assinatura deve igualmente ser atualizado.

1. Use o **comando show** a fim verificar os lugar atualmente configurados da assinatura.A saída mostra os lugar configurados da assinatura. Este comando mostra de onde as assinaturas running atuais são carregadas.`yourname#`**`show ip ips signatures`** `Builtin signatures are configured` As assinaturas foram carregadas por último de flash:128MB.sdfVersão de liberação S128.0 de Cisco SDFVersão de liberação V0.0 da tendência SDF
2. Use o **<url da cópia > os IP-sdf** comandam, junto com a informação da etapa precedente, a fim fundir arquivos de assinatura.`yourname#`**`copy tftp://10.10.10.5/mysignatures.xml ips-sdf`**
```
Loading mysignatures.xml from 10.10.10.5 (via Vlan1): ! [OK - 1612 bytes] *Oct 26
02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl No entry found
for lport 55577, fport 4714 No entry found for lport 51850, fport 4715 *Oct 26
02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
tftp://10.10.10.5/mysignatures.xml *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4
signatures - 1 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER -
there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-
ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines *Oct 26 02:43:34.920: %IPS-
6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new signature definitions for this
engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures - 3 of 15
engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are no new
signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING:
STRING.UDP - 17 signatures - 4 of 15 engines *Oct 26 02:43:34.920: %IPS-6-
ENGINE_BUILD_SKIPPED: STRING.UDP - there are no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures - 5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
This parameter is not supported *Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP -
2340 ms - packets for this engine will be scanned *Oct 26 02:43:37.288: %IPS-6-
ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15 engines *Oct 26 02:43:37.288: %IPS-6-
ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are no new
signature definitions for this engine *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING:
SERVICE.RPC - 29 signatures - 8 of 15 engines *Oct 26 02:43:37.288: %IPS-6-
ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are no new signature
definitions for this engine *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP -
132 signatures - 10 of 15 engines *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED:
SERVICE.HTTP - there are no new signature definitions for this engine *Oct 26 02:43:37.316:
%IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures - 11 of 15 engines *Oct 26 02:43:37.316:
%IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are no new signature definitions for this
engine *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures - 12 of 15
engines *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are no new
signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING:
ATOMIC.ICMP - 0 signatures - 13 of 15 engines *Oct 26 02:43:37.320: %IPS-6-
ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15
engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are no
new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING:
ATOMIC.L3.IP - 5 signatures - 15 of 15 engines *Oct 26 02:43:37.320: %IPS-6-
ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are no new signature definitions for this engine
yourname#
```
Depois que você emite o **comando copy**, o roteador carrega o arquivo de assinatura na memória e constrói então os Engine de assinatura. Na saída da mensagem do console SDEE, o estado da construção para cada Engine de assinatura é indicado.%IPS-6-ENGINE_BUILD_SKIPPED indica que não há nenhuma assinatura nova para este motor.%IPS-6-ENGINE_READY indica que há assinaturas novas e o motor está pronto. Como antes, o "15 mensagem de 15 motores" indica que todos os motores estiveram construídos.IPS-7-UNSUPPORTED_PARAM indica que um determinado parâmetro não está apoiado pelo Cisco IOS IPS. Por exemplo, CapturePacket e ResetAfterIdle.**Nota:** Estas mensagens são para a informação somente e não terão nenhuma influência na capacidade

ou no desempenho da assinatura IPS do Cisco IOS. Estes mensagens de registro podem ser desligados ajustando o nível de registro mais alto do que a eliminação de erros (nível 7).

3. Atualize o SDF definido pelo comando location da assinatura, tais que quando os recarregamentos de roteador, ele terão o grupo fundido da assinatura com assinaturas actualizados. Este exemplo mostra a diferença do tamanho do arquivo depois que a assinatura fundida salvar ao arquivo flash 128MB.sdf.`yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf yourname#`**`copy ips-sdf flash:128MB.sdf`** `yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf` **aviso:** O 128MB.sdf novo contém agora assinaturas cliente-fundidas. O índice é diferente do arquivo do padrão Cisco 128MB.sdf. Cisco recomenda que você muda este arquivo a um nome diferente para evitar a confusão. Se o nome é mudado, o comando location da assinatura precisa de ser mudado também.

Procedimento SDM 2.2

Depois que o Cisco IOS IPS foi permitido, as assinaturas novas podem ser adicionadas no roteador que executa um grupo da assinatura com a função da importação de Cisco SDM. Termine estas etapas a fim importar assinaturas novas:

1. Escolha o padrão SDFs ou o arquivo da atualização IOS-Sxxx.zip importar assinaturas adicionais.
2. O clique **configura**, e clica então a **prevenção de intrusão**.
3. Clique a aba **IPS da edição**, e clique então a **importação**.
4. Escolha do **PC da** lista de drop-down da importação.
5. Selecione o arquivo de que você quer importar assinaturas.Este exemplo usa a atualização a mais atrasada transferida do cisco.com e salvar no disco rígido do PC local.
6. Clique **aberto**.**aviso:** Devido ao confinamento de memória, somente um número limitado de assinaturas novas pode ser adicionado sobre as assinaturas que têm sido distribuídas já. Se assinaturas demais são selecionadas, o roteador não pôde poder carregar todas as assinaturas novas devido à falta de memória.Uma vez que a carga do arquivo de assinatura termina, a caixa de diálogo da importação IPS aparece.
7. Navegue com a vista de árvore esquerda, e clique a caixa de verificação da **importação** ao lado das assinaturas que você quer importar.
8. Clique o botão de rádio da **fusão**, e clique então a **APROVAÇÃO**.**Nota:** A opção da substituição substitui o grupo atual da assinatura no roteador com as assinaturas que você seleciona para importar.Uma vez que você clica a APROVAÇÃO, o aplicativo de Cisco SDM entrega as assinaturas ao roteador.**Nota:** A utilização elevada da CPU ocorre durante a compilação e a carga das assinaturas. Depois que o Cisco IOS IPS é permitido na relação, o arquivo de assinatura começa carregar. O roteador toma aproximadamente cinco minutos para carregar o SDF. Você pode tentar usar o **comando show process cpu** a fim ver a utilização CPU do Cisco IOS Software CLI. Contudo, não tente usar comandos adicionais ou carregar o outro SDFs quando o roteador carregar o SDF. Isto pode fazer com que o processo da compilação da assinatura tome mais por muito tempo para terminar (desde que a utilização CPU é próxima à utilização 100-percent na altura de carregar o SDF). Você pôde precisar de consultar através da lista de assinaturas e de permitir as assinaturas se não são estado dentro *permitido*.O número total da assinatura aumentou a 519. Este número inclui todas as assinaturas disponíveis no arquivo IOS-S193.zip que pertencem à subcategoria do compartilhamento de arquivo.

Para mais tópicos avançados sobre como usar Cisco SDM para controlar a característica IPS do Cisco IOS, refira a documentação de Cisco SDM nesta URL:

Selecione assinaturas e trabalhe com categorias da assinatura

A fim determinar como selecionar eficazmente as assinaturas corretas para uma rede, você deve conhecer algumas coisas sobre a rede que você está protegendo. Informação actualizado da categoria da assinatura em Cisco SDM 2.2 e nos clientes mais adicionais mais atrasados da assistência para selecionar o grupo correto de assinaturas para proteger a rede.

A categoria é uma maneira de agrupar assinaturas. Ajuda a reduzir para baixo a seleção da assinatura a um subconjunto das assinaturas que são relevantes entre si. Uma assinatura poderia pertencer a somente uma categoria ou poderia pertencer às categorias múltiplas.

Estas são as cinco categorias níveis mais alto:

- OS — categorização Operação-sistema-baseada da assinatura
- Ataque — categorização Ataque-baseada da assinatura
- Serviço — categorização Serviço-baseada da assinatura
- Protocolo da camada 2-4 — categorização Protocolo-nível-baseada da assinatura
- Liberações — categorização Liberação-baseada da assinatura

Cada um destas categorias é dividida mais em subcategorias.

Como um exemplo, considere uma rede home com uma conexão de faixa larga ao Internet e um túnel VPN à rede corporativa. O roteador de banda larga tem o Cisco IOS Firewall permitido na conexão (NON-VPN) aberta ao Internet de impedir que toda a conexão esteja originada do Internet e conectaa à rede home. Todo o tráfego que origina da rede home ao Internet é permitido. Supõe que o usuário usa um PC baseado em Windows e usa aplicativos como HTTP (navegação na web) e email.

O Firewall pode ser configurado de modo que somente os aplicativos que as necessidades de usuário estão permitidas correr através do roteador. Isto controlará o fluxo de tráfego indesejável e potencialmente ruim que pode espalhar durante todo a rede. Considere que o utilizador doméstico não precisa nem usa um serviço específico. Se esse serviço é permitido correr através do Firewall, há um furo potencial que um ataque possa usar para fluir durante todo a rede. Os melhores prática permitem somente os serviços que são precisados. Agora, é mais fácil selecionar que assinaturas a permitir. Você precisa de permitir assinaturas somente para os serviços que você reserva correr através do Firewall. Neste exemplo, os serviços incluem o email e o HTTP. Cisco SDM simplifica esta configuração.

A fim usar a categoria para selecionar assinaturas exigidas, escolha o **serviço > o HTTP**, e permita todas as assinaturas. Este processo de seleção igualmente trabalha no diálogo da importação da assinatura, onde você pode selecionar todas as assinaturas HTTP e as importar em seu roteador.

As categorias adicionais que precisam de ser selecionadas incluem o DNS, o NETBIOS/SMB, o HTTPS, e o S TP.

Assinaturas da atualização para arquivos do padrão SDF

O SDFs por-construído três (attack-drop.dsf, 128MB.sdf, e 256MB.sdf) é afixado atualmente no cisco.com em http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers somente). Umas versões mais novas destes arquivos serão afixadas assim que estiverem disponíveis. A fim atualizar o Roteadores que executa o Cisco IOS IPS com estes padrão SDFs,

vai ao Web site e transfere as versões as mais atrasadas destes arquivos.

Procedimento CLI

1. Copie os arquivos baixados ao lugar de onde o roteador é configurado para carregar estes arquivos. Para encontrar onde o roteador é configurado atualmente, use a executar-**configuração da mostra |** no comando do **sdf IP IP**.`Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave` Neste exemplo, o roteador usa 256MB.sdf no flash. O arquivo é atualizado quando você copia o 256MB.sdf transferido novo ao flash de roteador.
2. Recarregue o subsistema IPS do Cisco IOS para executar os arquivos novos.Há duas maneiras de recarregar o Cisco IOS IPS: recarregue o roteador ou reconfigure o Cisco IOS IPS para provocar o subsistema IO IPS para recarregar assinaturas. A fim reconfigurar o Cisco IOS IPS, remova todas as regras IPS das interfaces configuradas, e reaplique então as regras IPS de volta às relações. Isto provocará o sistema IPS do Cisco IOS para recarregar.

Procedimento SDM 2.2

Termine estas etapas a fim atualizar o padrão SDFs no roteador:

1. O clique **configura**, e clica então a **prevenção de intrusão**.
2. Clique a aba **IPS da edição**, e clique então **configurações globais**.A parte superior do UI mostra as configurações globais. A metade inferior do UI mostra lugar atualmente configurados SDF. Neste caso, o arquivo 256MB.sdf da memória Flash é configurado.
3. Escolha o **gerenciamento de arquivos do** menu de arquivo.A caixa de diálogo do gerenciamento de arquivos aparece.
4. **Arquivo da carga do** clique do **PC**.A caixa de diálogo do arquivo da salvaguarda aparece.
5. Escolha o SDF que precisa de ser atualizado, e clique **aberto**.O mensagem de advertência SDM aparece.
6. Clique **sim** a fim substituir o arquivo existente.Uma caixa de diálogo indica o progresso do processo da transferência de arquivo pela rede.
7. Uma vez que o processo da transferência de arquivo pela rede está completo, as **assinaturas do Reload do** clique localizaram na barra de ferramentas do lugar SDF. Esta ação recarrega o Cisco IOS IPS.**Nota:** O pacote IOS-Sxxx.zip contém todas as assinaturas que o Cisco IOS IPS apoia. As elevações a este pacote da assinatura estão afixadas no cisco.com assim que se tornarem disponíveis. A fim atualizar as assinaturas contidas neste pacote, veja Step2.

Informações Relacionadas

- Cisco Intrusion Prevention System
- Field Notice de produto de segurança (que incluem a intrusion detection do CiscoSecure)
- Suporte Técnico - Cisco Systems