Formato da assinatura da versão do sistema 4.x da prevenção de intrusão ao exemplo de migração do formato da assinatura da versão 5.x

Índice

Introdução

No ® do Cisco IOS libere 12.4(11)T e mais tarde, o Cisco IOS Intrusion Prevention System (IPS) fornece o apoio para o formato da assinatura da versão de software 5.x do ips Cisco. O formato da assinatura 5.x é um formato versão-baseado da definição XML da assinatura igualmente usado pelo outro Produtos dispositivo-baseado Cisco IPS. O apoio para assinaturas e arquivos de definição da assinatura (SDFs) na versão 4.x do ips Cisco é interrompido no este e em uns software release mais adicionais do T-trem do Cisco IOS.

Os clientes que executam o Cisco IOS IPS com formato SDFs da assinatura da versão 4.x podem reconfigurar o Cisco IOS IPS para usar categorias predefinidas Cisco da assinatura, grupos básicos e avançados da assinatura, ou a utilidade da migração IPS do Cisco IOS a fim migrar arquivos da versão anterior 4.x SDF na versão 5.x do ips Cisco formatam grupos da assinatura.

Este documento descreve como migrar de um formato SDF do ips Cisco 4.x e permitir a assinatura migrada ajustada no Cisco IOS Release 12.4(11)T ou Mais Recente. Para obter mais informações sobre de como configurar o Cisco IOS IPS no Cisco IOS Release 12.4(11)T ou Mais Recente, refira realces do apoio e da usabilidade do formato da assinatura IPS 5.x.

Nota: Cisco recomenda que você executa a migração IPS do Cisco IOS antes que você promova a uma imagem do Cisco IOS Release 12.4(11)T ou Mais Recente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Cisco IOS Release 12.4(11)T ou Mais Recente.

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.

Etapas para migrar arquivos da versão 4.x SDF

O script da migração exige um arquivo do formato SDF do ips Cisco 4.x e (opcionalmente) o arquivo de configuração de CLI que contém a informação de configuração IPS do Cisco IOS usada em uma liberação do thatrunsa do roteador mais cedo do que o Cisco IOS Release 12.4(11)T.

O script da migração procura pelos comandos que contêm o **<sigid > o [<sigsubid>] da assinatura IP IP desabilitados** dentro do arquivo de configuração de roteador. Se o arquivo de configuração não contém este comando CLI, não há nenhuma necessidade para que o script da migração leia o arquivo de configuração de CLI. A conversão das assinaturas, é baseada como tal unicamente no SDF.

Se você executa o script da migração antes que você promova o Cisco IOS IPS ao Cisco IOS Release 12.4(11)T ou Mais Recente, siga o processo executam dentro o script da migração IPS do Cisco IOS.

Se você executa o script da migração depois que você promove o Cisco IOS IPS ao Cisco IOS Release 12.4(11)T ou Mais Recente, termine estas etapas:

1. Verifique toda a necessidade de converter os comandos CLI, **<sigid da assinatura IP IP > [<sigsubid>] desabilitados**, como mencionado acima.
2. Use o **flash da executar-configuração do** comando copy**: ipscfg.cfg a fim** salvar a configuração de CLI do roteador a um arquivo.Este comando suporta a configuração do roteador existente para piscar em um arquivo nomeado *ipscfg.cfg.* O processo de migração usa este arquivo para 4.x completo à conversão do formato da assinatura 5.x.
3. Continue executar o script da migração IPS do Cisco IOS.

Execute o script da migração IPS do Cisco IOS

O script da migração está disponível do cisco.com nesta URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Salvar o script da migração ao flash do roteador ou a um lugar roteador-acessível, tal como um server do Trivial File Transfer Protocol (TFTP).

O script da migração converte um SDF do formato da versão 4.x do ips Cisco ao formato da versão 5.x. O script da migração apoia somente estes parâmetros da assinatura:

- severidade
- ação
- habilitado

Além, o script da migração pode igualmente ler de um fileand da configuração IO IPS migra as assinaturas deficientes que foram configuradas pelo comando **desabilitado <sigsubid> do <sigid> da assinatura** CLI **IP IP nas** liberações mais cedo do que o Cisco IOS Release 12.4(11)T.

Nota: (Não as assinaturas feitas sob encomenda de Cisco) não são convertidas com este script.

Este exemplo mostra como migrar o arquivo formatado 4.x *sdmips.sdf* IPS ao Cisco IOS IPS no Cisco IOS Release 12.4(11)T com apoio do formato da assinatura IPS 5.x do Cisco IOS.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
     from 4.x format to 5.x format.
The migration script will migrate only the following signature
     parameters - severity, action, enabled - for Cisco (non-custom) signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
  flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
     choice: flash:// sdmips.sdf
Migrating following SDF file (this will a take few minutes):
  flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
  C2821-sigdef-delta.xml
C2821#
```

Primeiramente, o script da migração indica um breve texto sobre sua função. Em seguida, o script fornece uma opção para escolher um lugar de onde ler a configuração atual (da PRE-migração) para o Cisco IOS IPS. O padrão lê da configuração de inicialização. Se você salvar previamente uma configuração a um servidor TFTP ou ao flash do roteador, especifique o lugar na alerta.

Por exemplo:

Use a *configuração de CLI de* **tftp:// 192.168.1.5/<router >** a fim notificar o script para carregar uma configuração de CLI do servidor TFTP 192.168.1.5.

Use a <saved-**configuração de flash:// >** a fim ler de um arquivo salvar no flash.

Carregue as assinaturas migradas no Cisco IOS IPS no Cisco IOS Software Release 12.4(11)T

Depois que a migração da assinatura está completa, promova a imagem do roteador ao Cisco IOS Release12.4(11)T se você já não fez assim. Uma vez que o roteador é recarregado, termine estas etapas.

1. Permita o Cisco IOS IPS.Esta saída mostra como permitir o Cisco IOS IPS em um Cisco 2821 Router. Para obter mais informações sobre de como configurar o Cisco IOS IPS, refira

realces do apoio e da usabilidade do formato da assinatura IPS 5.x.
```
C2821#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```

2. A cópia e cola esta chave no roteador a fim configurar a chave pública cripto da assinatura.
```
C2821#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```

3. Permita o Cisco IOS IPS em relações segundo as indicações deste exemplo:
```
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```

4. Use o **comando copy** a fim carregar o pacote o mais atrasado da assinatura:
```
C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
```
Este comando carrega assinaturas do pacote *IOS-S253-CLI.pkg da* assinatura no Cisco IOS IPS.**Nota: a categoria toda da assinatura IO-IP** foi configurada em etapa 1, que se aposenta todas as assinaturas. Depois que o pacote da assinatura é carregado com sucesso, nenhuma assinatura está selecionada e compilada.

5. Use este comando a fim carregar o arquivo migrado XML ao Cisco IOS IPS:**<router-hostname >-sigdef-delta.xml**Por exemplo:
```
copy flash:C2821-sigdef-delta.xml idconf
```
Uma vez que o roteador analisa gramaticalmente o arquivo de assinatura formatado versão 5.x, a migração está completa.

6. Use o **comando count da assinatura da mostra IP IP** a fim verificar o status sumário da assinatura, e use então os **detalhes da assinatura da mostra IP IP** comandam a fim ver detalhes específicos em todas as assinaturas.

Informações Relacionadas

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