Compreenda como a característica automática da atualização de assinatura do ips Cisco trabalha

Índice

Introdução

Este documento fornece uma vista geral da característica automática da atualização do Sistema de prevenção de intrusões da Cisco (IPS) e de sua operação.

A característica automática da atualização IPS foi introduzida na versão 6.1 IPS e fornece administradores uma maneira fácil atualizar assinaturas IPS em um intervalo regularmente programado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- As atualizações de assinatura exigem uma assinatura e uma chave de licença válidas dos Serviços Cisco para IPS. Vá a http://www.cisco.com/go/license e clique o **serviço da assinatura da assinatura IPS** a fim aplicar-se para uma chave de licença.
- Uma conta de usuário de Cisco.com (CCO) que seja associada com uma assinatura ativa dos Serviços Cisco para IPS.
- Privilégios transferir o software criptográfico. Ir para: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y a fim verificar se você tem o acesso.

Componentes Utilizados

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

- Versões 6.1 e mais recente do ips Cisco
- Características específicas para versões 7.2(1) do ips Cisco, 7.3(1), e mais tarde

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.

Informações de Apoio

Requisitos de Rede

1. O comando e a interface de controle do IPS exigem de acesso direto ao Internet usando HTTPS (TCP 443) e HTTP (TCP 80).
2. O Network Address Translation (NAT) e o Access Control Lists (ACLs) em dispositivos de ponta tais como o Roteadores e os Firewall precisam de ser configurados a fim permitir a Conectividade IPS ao Internet.
3. Exclua o comando e o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de controle de todos os filtros do índice e shapers do tráfego de rede.
4. Os servidores proxy automáticos dos suportes de recurso da atualização 7.2(1) na liberação certificada FIPS/CC. Todos software release 6.x e 7.x restantes não apoiam a atualização

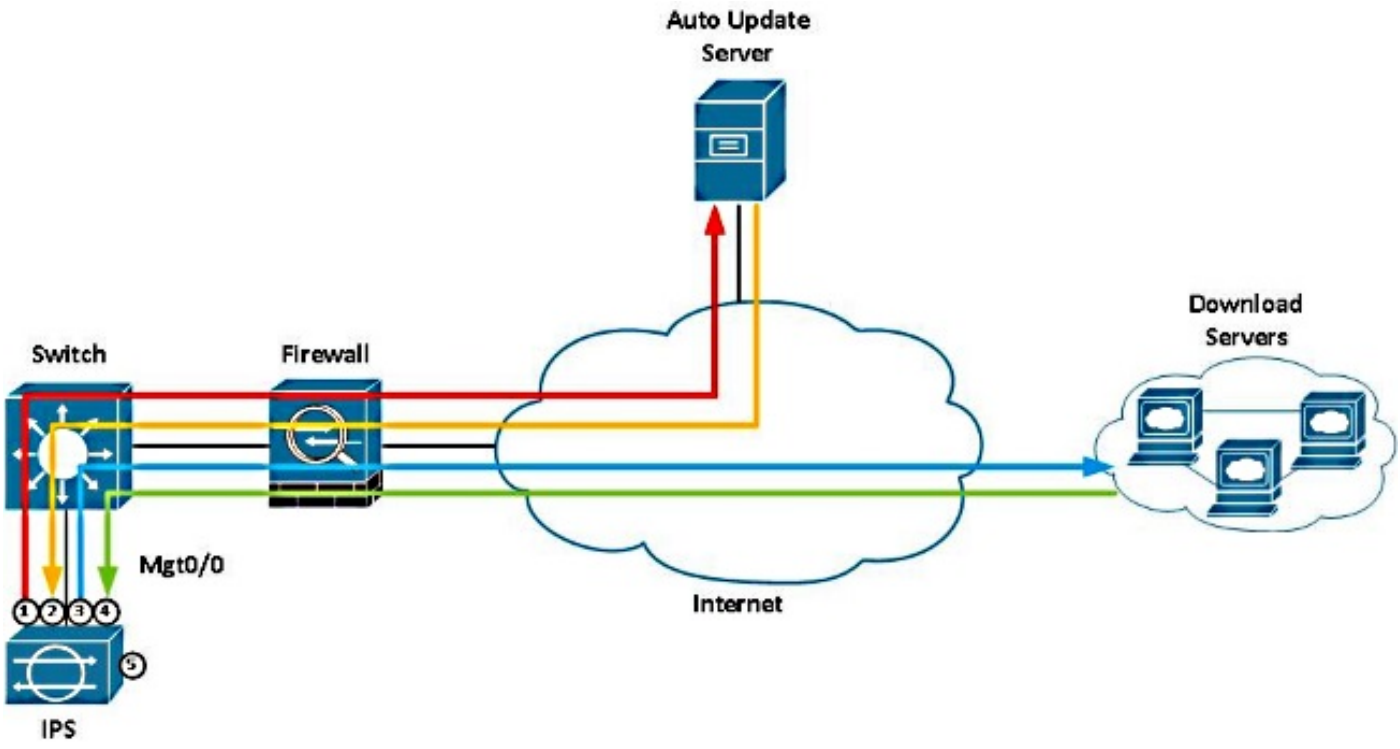
automática através de um servidor proxy neste tempo. 7.2(1) A liberação inclui um número de mudanças ao Shell Seguro (ssh) do padrão e aos ajustes HTTPS. Refira Release Note para o Sistema de prevenção de intrusões da Cisco 7.2(1)E4 antes que você promova a 7.2(1).

aviso: Na versão 7.0(8)E4 do ips Cisco, o valor padrão para o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Cisco é mudado de 198.133.219.25 a 72.163.4.161 na auto configuração da atualização URL. Se seu sensor é configurado para atualizações automáticas, você pôde precisar de atualizar as regras do Firewall a fim permitir que o sensor conecte ao endereço IP de Um ou Mais Servidores Cisco ICM NT novo. Para versões 7.2 e mais recente do ips Cisco, o endereço IP do servidor automático codificado da atualização é substituído com um Nome de domínio totalmente qualificado Nomeado (FQDN) e a consulta do Domain Name System (DNS). Refira a seção de configuração deste documento para a informação adicional.

Contorneie advertências

Algumas atualizações de assinatura exigem as tabelas da expressão regular ser recompiled durante que a hora o IPS pode entrar no modo de desvio do software. Para sensores inline com o modo de desvio ajustado ao automóvel, o motor da análise é contorneado permitindo que o tráfego corra através das relações inline e dos pares inline VLAN sem inspeção. Se o modo de desvio é ajustado a fora, o sensor inline para de passar o tráfego quando a atualização for aplicada.

Processo de atualização do automóvel da assinatura



1. O IPS autentica ao Auto Update Server em 72.163.4.161 usando HTTPS (TCP 443).

2. O IPS envia um cliente manifesto ao Auto Update Server, que inclua a plataforma ID e um segredo compartilhado cifrado que o server se use para verificar a autenticidade do sensor do ips Cisco.

3. Uma vez que autenticado, o server da atualização responde com um server manifesto que contenha uma lista de opções de arquivo da transferência associadas com a plataforma ID. Os dados contidos aqui incluem relativo à informação para atualizar a versão, a localização do download, e protocolos de transferência de arquivo apoiados. Baseado nestes dados, lógica da atualização IPS a auto determina se algumas das opções da transferência são válidas e selecionam então o melhor pacote da atualização para a transferência. À vista da transferência, o server fornece o IPS um grupo de chaves a ser usadas para decifrar o arquivo da atualização.

4. O IPS estabelece uma nova conexão ao server da transferência identificado no server manifesto. O endereço IP do servidor da transferência varia, que é dependente do lugar. O IPS usa o protocolo de transferência de arquivo definido nos dados URL da transferência do arquivo aprendidos no server manifesto (atualmente usos HTTP (TCP 80)).

5. O IPS usa as chaves previamente transferidas para decifrar o pacote da atualização e aplica então os arquivos de assinatura ao sensor.

Configurar

Configuração básica da atualização automática da assinatura

A característica automática da atualização pode ser configurada do gerenciador de dispositivo IPS (IDM) ou do gerente IPS expresso (IME). Conclua estes passos:

1. De IDM/IME, escolha a **configuração > o Gerenciamento do sensor > a atualização do automóvel/cisco.com.**