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.**

2. Escolha as **atualizações da assinatura e do motor da possibilidade da** caixa de verificação do **cisco.com no** painel direito, e clique sobre o título azul das **configurações de servidor de Cisco.com** a fim deixar cair para baixo a placa da configuração.

3. Incorpore o nome de usuário e senha CCO.

   Está aqui um exemplo URL para versões 7.0(8) e 7.1(6) do ips Cisco:

   https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl

   Está aqui um exemplo URL para versões 7.2(1) do ips Cisco, 7.3(1), e mais tarde:

   https://www.cisco.com//cgi-bin/front.x/ida/locator/locator.pl

   Note: Não mude o cisco.com URL. Não deve precisar de ser mudado de sua configuração padrão. //é intencional e não um erro tipográfico. Em versões 7.2(1) do ips Cisco, 7.3(1), e mais tarde, o sensor perguntam o servidor DNS que é definido na configuração de rede do sensor a fim resolver www.cisco.com URL a um endereço IP roteável de Internet.

4. Configurar umas horas inicial e uma frequência a fim programar a atualização de assinatura. Recomenda-se ajustar as horas inicial a um tempo aleatório que não esteja na parte superior da hora. Neste exemplo, a hora é ajustada a 23:15:00. A frequência pode ser configurada para apoiar de hora em hora ou a atualização diária tenta. O clique **aplica-se** a fim aplicar alterações de configuração.

Realces automáticos da atualização da assinatura

Muitas melhorias à característica automática da atualização são incluídas em versões 7.2(1) e mais recente do ips Cisco. As melhorias da segurança adicional são adicionadas igualmente às versões 7.3(2) e mais recente do ips Cisco. Refira as opções de configuração descritas nesta seção para a informação adicional.

Atualize agora a característica

A versão 7.2(1) do ips Cisco introduziu uma capacidade nova ao IPS GUI e o CLI que permite que os administradores iniciem uma atualização automática da assinatura imediatamente, que contorneie a necessidade de esperar o tempo agendado ocorrer.

A fim contornear imediatamente a programação da atualização e a atualização automáticas, navegue ao IDM/IME e escolha a **configuração > o Gerenciamento do sensor > a atualização do automóvel/cisco.com. Enquanto** a atualização automática corretamente é configurada e aplicada, você pode clicar o **botão de** UpdateNow no canto direito superior da tela a fim provocar uma tentativa da atualização.

Você pode igualmente incorporar o comando do **autoupdatenow no** sensor CLI a fim provocar uma tentativa da atualização. Aqui está um exemplo:

```
SSP-60# autoupdatenow
Warning: Executing this command will perform an auto-upgrade on the sensor immediately.
Before executing this command, you must have a valid license to apply the Signature
AutoUpdates and auto-upgrade settings configured.After executing this command please
disable user-server/cisco-server inside 'auto-upgrade' settings, if you don't want
scheduled auto-updates
Continue? []: yes
Automatic Update for the sensor has been executed.Use 'show statistics host' command
to check the result of auto-update.Please disable user-server/cisco-server in
auto-upgrade settings, if you don't want scheduled auto-updates
```

Atualização automática através do proxy do Internet

A fim provocar uma atualização automática através do proxy do Internet, navegue ao IDM/IME e escolha a **configuração > o sensor Setup > rede**. Entre no DNS e (opcionalmente) no endereço IP de Um ou Mais Servidores Cisco ICM NT e na porta do servidor proxy HTTP:

Valide Certificados do root confiável

A versão 7.3(2) do ips Cisco introduziu a capacidade para que o IPS valide a corrente de certificado de raiz do server do updater quando as atualizações são transferidas. Com esta característica permitida, o IPS valida se o certificado de raiz no certificate chain está assinado por um root confiável CA por exemplo, os certificados de raiz TLS que são obtidos no processo da atualização de assinatura do servidor Cisco e o server global da correlação é validado. Esta característica é desabilitada atualmente à revelia na versão 7.3(2) do ips Cisco; contudo, pôde ser permitida à revelia em uma liberação futura. Refira o IPS *leem-me* arquivo para mais informação.

Veja a loja local do certificado confiável

A fim ver a lista atual de Certificados instalados do root confiável em versões 7.3(2) e mais recente IPS, navegue à **configuração > ao Gerenciamento do sensor > aos Certificados > aos Certificados do root confiável**:

Permita a validação restrita do certificado de servidor TLS

Termine estas etapas a fim permitir a característica restrita da validação do server TLS:

1. Navegue à **configuração > ao sensor Setup > rede**.
2. Expanda o **HTTP, o FTP, o telnet, o SSH, o CLI & as outras opções** deixam cair para baixo o menu.
3. Verifique a caixa de verificação **restrita da validação do server da possibilidade TLS**.
4. O clique **aplica-se** a fim aplicar a configuração ao sensor.

Adicionar/certificados de raiz da atualização à loja local do certificado confiável

Enquanto os Certificados expiram nos server do updater, Cisco reserva o direito de usar uma corrente de certificado de raiz a não ser GeoTrust e Thawte. Se o certificado actualizado não existe na imagem do software atual IPS, a seguir a corrente de certificado de raiz actualizado pode manualmente ser instalada na loja local do certificado confiável do sensor. Os Certificados DER-codificados podem ser posicionados sobre um servidor de arquivo e ser recuperados pelo sensor através do SCP ou do HTTPS. O exemplo seguinte usa o SCP a fim demonstrar a instalação certificada/processo de atualização.

1. Do IDM/IME, navegue à **configuração > ao Gerenciamento do sensor > ao SSH > chaves conhecidas do host RSA**.
2. O clique **adiciona** e incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT do server SCP.
3. O clique **recupera a chave Host** a fim mandar o sensor automaticamente recuperar a chave pública do server.
4. Clique a **APROVAÇÃO** duas vezes e **aplique-a** então a fim aplicar a configuração ao sensor. **Note**: Um aviso aparece se o tamanho chave apresentado pelo server SCP é menor de 2,048 bit.
5. O clique **sim** a fim adicionar a chave aos anfitriões conhecidos apresenta ou **nenhum** a fim retornar à tela **conhecida adicionar da chave do host RSA**.
6. Navegue aos **Certificados da configuração > do Gerenciamento > do root confiável do sensor**.

7. O clique **adiciona/atualização** a fim adicionar um arquivo certificado DER-codificado novo do server SCP. Assegure-se de que o arquivo certificado prepositioned no server e disponível para a recuperação remota através do SSH.

8. Selecione o **SCP** como o protocolo e incorpore a URL, o username, e a senha.

9. Clique a **APROVAÇÃO** a fim começar transferência e a instalação de arquivo certificado.

10. Clique **sim** a fim adicionar o certificado à loja local do root confiável IPS e **APROVAÇÃO** a fim retirá-lo então.

Verificar

Do IDM/IME, escolha a **configuração > o Gerenciamento do sensor > a atualização do automóvel/cisco.com. Expanda a seção de informação de** AutoUpdate a fim rever o estado da última tentativa da transferência. **Clique a** ordem de Refreshin para refrescar os **dados da informação de** AutoUpdate.

A fim verificar o estado do processo de atualização automático através do CLI, inscreva o **comando host das estatísticas da mostra**:

```
IPS# show statistics host
<Output truncated>
Auto Update Statistics
lastDirectoryReadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Read directory: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
= Success
lastDownloadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Download: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
IPS-sig-S654-req-E4.pkg
= Success
nextAttempt = 17:55:00 GMT-06:00 Wed Jun 27 2012
lastInstallAttempt = 16:55:46 GMT-06:00 Wed Jun 27 2012
= Success
<Output truncated>
```

Do IDM/IME, refira o dispositivo licenciar no painel home a fim ver o estado da licença e a versão da assinatura atualmente instalada. A mesma informação pode ser obtida através do CLI com o **comando show version**.

```
SSP-60# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(2)E4

Host:
Realm Keys key1.0
Signature Definition:
Signature Update S805.0 2014-06-03
Threat Profile Version 7
OS Version: 2.6.29.1
```

```
Platform: ASA5585-SSP-IPS60
Serial Number: JAF1527CPNK
Licensed, expires: 21-Jun-2014 UTC
Sensor up-time is 39 days.
Using 46548M out of 48259M bytes of available memory (96% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 86.6M out of 377.5M bytes of available disk space (24% usage)
boot is using 63.4M out of 70.5M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
AnalysisEngine C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CollaborationApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CLI C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500

Upgrade History:

* IPS-sig-S802-req-E4 16:07:23 UTC Thu May 29 2014
IPS-sig-S805-req-E4.pkg 16:18:51 UTC Mon Jun 09 2014

Recovery Partition Version 1.1 - 7.3(2)E4

Host Certificate Valid from: 15-Jul-2013 to 16-Jul-2015
```

Troubleshooting

Após a configuração correta da auto atualização de assinatura, termine estas etapas a fim isolar e corrigir edições geralmente encontradas:

1. Para todos os dispositivos e módulos IPS à exceção de AIM e do IDSM, assegure-se de que o comando e a interface de controle estejam conectados à rede local, atribuída um endereço IP válido/máscara de sub-rede/gateway, e tenham o IP reachability ao Internet. Para os módulos de AIM e IDSM, o comando virtual e a interface de controle são utilizados como definido na configuração. A fim confirmar o status operacional da relação do CLI, inscreva este **comando show**:

   ```
   IPS# show interfaces
   <Output truncated>
   MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description = Media Type = TX
   Default Vlan = 0
   Link Status = Up <---
   <Output truncated>
   ```

2. A fim validar se a conta de usuário de CCO tem privilégios necessários transferir pacotes da atualização de assinatura, abra um navegador da Web e um início de uma sessão ao cisco.com com esta mesma conta CCO. Uma vez que autenticado, transfira manualmente o pacote o mais atrasado da assinatura IPS. A incapacidade transferir manualmente o pacote é provavelmente devido a à falta da associação da conta de usuário a uma assinatura válida dos Serviços Cisco para IPS. Além, o acesso ao software de segurança no CCO é

restringido aos usuários autorizados que aceitaram o acordo anual da criptografia/exportação. A falha aprovar este acordo foi sabida impedir transferências da assinatura de IDM/IME/CSM. A fim verificar se este acordo esteve aceitado, abra um navegador e um início de uma sessão ao cisco.com com a mesma conta CCO. Uma vez que autenticado, tente transferir manualmente o Cisco IOS? pacote de softwares com o conjunto de recursos K9.

3. Verifique se há um proxy no lugar para o tráfego encadernado do Internet (todas as versões exceto 7.2(1) e mais atrasado). Se o tráfego do comando e da porta de controle atravessa este proxy, a auto característica da atualização não trabalha. Reconfigure a rede de modo que o comando e o tráfego da porta de controle não sejam filtrados com um proxy e teste-a outra vez.

4. Para os sensores que executam versões 7.2 ou 7.3 software, assegure-se de que uns ou vários servidores DNS estejam configurados. Isto é exigido de modo que o sensor possa resolver o FQDN do updater de www.cisco.com a um endereço IP roteável de Internet.

5. Verifique se há algum filtragem de conteúdo ou aplicativo ou dispositivo do modelagem de tráfego no trajeto ao Internet. Se o presente, configura uma exclusão a fim permitir o endereço IP de Um ou Mais Servidores Cisco ICM NT do comando e da interface de controle alcançar o Internet sem limitação.

6. Se o tráfego ICMP é permitido para o Internet, abra o CLI do sensor IPS e tente-o sibilar um endereço IP público.

   Este teste pode ser usado para verificar se o roteamento necessário e as regras NAT (se usado) são configurados corretamente. Se o teste ICMP sucede contudo as auto atualizações continuam a falhar, assegure-se de que os dispositivos de rede tais como o Roteadores e os Firewall ao longo do trajeto permitam o HTTPS e as sessões de HTTP do IP do comando e da interface de controle IPS. Por exemplo, se o endereço IP de Um ou Mais Servidores Cisco ICM NT do comando e do controle é 10.1.1.1, uma entrada ACL simples em um Firewall ASA pode olhar como este exemplo:

```
IPS# show interfaces
<Output truncated>
MAC statistics from interface Management0/0
Interface function = Command-control interface
Description = Media Type = TX
Default Vlan = 0
Link Status = Up <---
<Output truncated>
```

7. O username CCO não deve conter nenhuns caracteres especiais, por exemplo, @. Refira a identificação de bug Cisco CSCsq30139 para mais informação.

8. Quando as falhas da atualização automática da assinatura ocorrem, use a tabela seguinte a fim combinar os códigos de erro de HTTP associados.

```
IPS# show statistics host
Auto Update Statistics
lastDirectoryReadAttempt = 19:31:09 CST Thu Nov 18 2010
= Read directory: https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl
= Error: AutoUpdate exception: HTTP connection failed [1,110] <--
lastDownloadAttempt = 19:08:10 CST Thu Nov 18 2010
lastInstallAttempt = 19:08:44 CST Thu Nov 18 2010
nextAttempt = 19:35:00 CST Thu Nov 18 2010
```

Mensagem	Significado
Erro: Exceção de AutoUpdate: [1,110] falhado conexão de HTTP	Autenticação falhada. Verifique o nome de usuário e senha.
exceção de AutoUpdate do status=false: Receba [3,212] falhado resposta HTTP	O pedido ao Auto Update Server cronometrado para fora.
Erro: resposta de erro de HTTP: 400	Certifique-se que o ajuste Cisco-URL está optado. Se o ID de CCO é maior de 32 caráter comprimento, tente um ID de CCO diferente. Esta pode ser uma limitação no server da transferência de Cisco.
Erro: Exceção de AutoUpdate: [1,0] falhado conexão de HTTP	A transferência impedida questão de rede ou lá é um problema potencial com os server da transferência.