知道思科IPS自动签名更新功能如何运作

目录

简介

本文提供思科入侵防御系统(IPS)自动更新功能和其操作的概述。

IPS自动更新功能在IPS版本6.1介绍并且提供管理员简单的方法更新在一个有规律地被安排的间隔的IPS签名。

先决条件

要求

Cisco 建议您了解以下主题：

- 签名更新要求一个有效Cisco Services for IPS订阅和许可证密钥。 去http://www.cisco.com/go/license并且点击**IPS签名订阅服务**为了申请许可证密钥。

- 关联与一活动Cisco Services for IPS订阅的Cisco.com (CCO)用户帐户。
- 权限下载加密软件。 去对： http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y为了检查是否访问。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- Cisco IPS版本6.1和以上
- Cisco IPS版本7.2(1)， 7.3(1)和以后的特定功能

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

网络要求

1. 使用HTTPS (TCP 443)和HTTP (TCP 80)， IPS的命令和控制接口要求直接访问到互联网。
2. 网络地址转换(NAT)和访问控制列表(ACL)在边缘设备例如路由器和防火墙需要配置为了允许IPS连接到互联网。
3. 从所有内容过滤器和网络流量成型机屏蔽命令和控制接口IP地址。
4. 在7.2(1) FIPS/CC被证实的版本的自动更新功能支持代理服务器。其他6.x和7.x软件版本不通过代理服务器支持自动更新此时。7.2(1)版本包括对默认安全壳SSH和HTTPS设置的一定数量的更改。 思科入侵防御系统的7.2(1)E4参考的版本注释，在您升级到7.2(1)前。

   警告：在Cisco IPS版本7.0(8)E4， Cisco服务器IP地址的默认值从198.133.219.25在自动更新URL配置里更改到72.163.4.161。如果您的传感器为自动更新配置，您也许需要更新防火墙规则为了允许传感器连接到新的IP地址。对于Cisco IPS版本7.2和以上，硬编码的自动更新服务器IP地址用已命名完全合格的域名(FQDN)和域名系统(DNS)查找替换。参考本文配置部分其他信息。

旁路警告

在IPS可以进入软件旁路模式期间，一些签名更新要求将重新编译的常规表示表。对于轴向传感器旁路模式设置为自动，绕过允许流量的分析引擎流经轴向接口和轴向VLAN对，不用检查。 如果旁路模式设置对，轴向传感器停止通过流量，当更新应用时。

签名自动更新过程

1. 使用HTTPS (TCP 443)， IPS验证到Auto Update服务器在72.163.4.161。

2. IPS派遣明显的客户端到Auto Update服务器，包括平台ID和一已加密共享机密服务器使用验证思科IPS传感器的真实性。

3. 一旦验证，更新服务器回应包含下载文件选项列表关联与平台ID明显的服务器。包含的数据此处包括相关的信息更新版本、下载位置和支持的文件传输协议。凭此数据， IPS自动更新逻辑确定其中任一个下载选项是否有效然后选择下载的最好的更新包。为准备下载，服务器提供IPS将使用的一套密钥解密更新文件。

4. IPS在明显的服务器建立对识别的下载服务器的一个新连接。下载服务器IP地址变化，依靠位置。IPS在服务器了解的文件下载数据URL使用定义的文件传输协议明显(当前用途HTTP (TCP 80))。

5. IPS使用以前下载的密钥解密更新包然后适用于签名文件传感器。

配置

基本签名Auto-update配置

自动更新功能可以从IPS设备管理器(IDM)或IPS管理器Express (IME)配置。完成这些步骤：

1. 从IDM/IME，请选择**Configuration>传感器Management>自动/Cisco.com更新。**

2. **从**在右边的窗格的**Cisco.com**复选框选择**Enable (event)签名和引擎更新**，并且点击蓝色**Cisco.com服务器设置**标题为了下降下来配置窗格。

3. 输入CCO用户名和密码。

   这是Cisco IPS版本7.0(8)和7.1(6)的示例URL ：

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

   这是Cisco IPS版本7.2(1)， 7.3(1)和以后的示例URL ：

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

   注意：请勿更改Cisco.com URL。它不应该需要从其默认设置更改。//是故意而不是印刷错误。在Cisco IPS版本7.2(1)， 7.3(1)和以后，传感器查询在传感器网络配置里定义为了解决

www.cisco.com URL到互联网可路由IP地址的DNS服务器。

4. 配置开始时间和频率为了安排签名更新。推荐设置开始时间为不在小时的上面的随机时间。 在本例中，时刻设置到23:15:00。 频率可以配置支持每小时或每天更新尝试。单击**应用**为了应用配置更改。

签名自动更新增强

对自动更新功能的许多改进在Cisco IPS版本7.2(1)和以上包括。附加安全性改进也被添加到Cisco IPS版本7.3(2)和以上。 参考在此部分描述的配置选项其他信息。

更新当前以为特色

Cisco IPS版本7.2(1)介绍允许管理员立即启动签名自动更新，绕过需要等待预定时间发生的一个新的功能对IPS Guis和CLI。

为了绕过自动更新请立即安排并且更新，导航对IDM/IME并且选择**Configuration>传感器Management>自动/Cisco.com更新。 只要**自动更新正确地配置并且应用，您能点击在屏幕的右上角的UpdateNow**按钮**为了触发更新尝试。

您能也输入**autoupdatenow**命令到传感器CLI为了触发更新尝试。示例如下：

```
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
```

自动更新通过互联网代理

为了通过互联网代理触发一次自动更新，请导航对IDM/IME并且选择**设置的Configuration>传感器>网络**。输入DNS和(或者) HTTP代理服务器IP地址和端口：

验证可信的根证书

当更新下载时， Cisco IPS版本7.3(2)介绍IPS的能力能验证更新服务器的根证明一系列。启用此功能， IPS验证根证明在证书链是否由可信的根例如CA.签字，在签名更新进程获取从思科服务器，并且全局相关性服务器验证的TLS根证明。默认情况下此功能在Cisco IPS版本7.3(2)当前禁用;默认情况下然而，它在以后的版本也许启用。 参考IPS*读我*文件欲知更多信息。

查看本地信任证书存储

为了查看已安装可信的根证书当前列表在IPS版本7.3(2)和以上的，导航对**Configuration>传感器Management>证书>可信的根证书**：

Enable (event)严格TLS服务器证书验证

完成这些步骤为了启用严格TLS服务器验证功能：

1. 导航对**设置的Configuration>传感器>网络**。
2. 展开**HTTP、FTP，Telnet、SSH、CLI &其它选项**下拉菜单。
3. 检查**Enable (event)严格TLS服务器验证**复选框。
4. 单击**应用**为了适用于配置传感器。

添加/对本地信任证书存储的更新根证明

当证书在更新服务器超时，除GeoTrust和Thawte之外，思科保留权利使用根证明一系列。如果更新证书在当前IPS软件镜像不存在，则更新根证明一系列可以手工安装到传感器的本地信任证书存储。DER编码的证书在文件服务器可以被安置和由传感器获取通过SCP或HTTPS。下一个示例使用SCP为了展示认证安装/更新过程。

1. 从IDM/IME，请导航对**Configuration>传感器Management> SSH >已知主机RSA密钥**。
2. 单击**添加**并且输入SCP服务器的IP地址。
3. 单击自动地**获取主机密钥**为了安排传感器从服务器获取公共密钥。
4. 两次点击OK键然后**应用**为了适用于配置传感器。 **注意**：如果SCP服务器提交的密钥大小小于2,048个位，警告出现。
5. 点击**是**为了添加密钥到已知主机表或**没有**为了返回到**添加已知主机RSA密钥**屏幕。
6. 导航对**Configuration>传感器Management>可信的根证书**。
7. 单击**添加/更新**为了从SCP服务器添加新的DER编码的证书文件。保证证书文件在服务器和联机被前置远程检索的通过SSH。
8. 选择**SCP**作为协议并且输入URL、用户名和密码。
9. 点击OK键为了开始证书文件传输和安装。
10. 点击**是**为了添加证书到IPS本地可信的根存储**OK**为了然后退出。

验证

从IDM/IME，请选择**Configuration>传感器Management>自动/Cisco.com更新。展开**自动更新**信息部分**为了查看最后下载尝试的状况。 **点击**Refreshin定货刷新自动更新**信息数据**。

为了通过CLI验证自动更新过程的状况，请输入**host命令的show statistics** ：

```
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>
```

从IDM/IME，参考在家庭控制板的许可授权的小配件为了查看许可证状态和当前安装签名版本。同一信息可以通过CLI得到用**show version命令**。

```
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
```

故障排除

在自动签名更新的正确配置以后，请完成这些步骤为了查出和修改通常遇到的问题：

1. 对于所有IPS设备和模块除了AIM和IDSM，请保证命令和控制接口连接对本地网络，分配有效IP地址/子网掩码/网关，并且有IP可达性到互联网。对于AIM和IDSM模块， virtual命令和控制接口使用如对配置定义。为了证实接口的运行状态从CLI的，请输入此**show命令**：

   ```
   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. 为了验证CCO用户帐户是否有必要的权限下载签名更新包，请打开Web浏览器并且登陆对与此同样CCO帐户的Cisco.com。一旦验证，请手工下载最新的IPS签名包。手工下载包的无法可能归结于缺乏用户帐户的关联对一有效Cisco Services for IPS订阅。另外，对security software的访问在CCO限制给接受每年加密/出口协议的授权用户。疏忽审批此协议被认识防止签名下载IDM/IME/CSM。为了验证此协议是否接受，请打开浏览器和登录对与同一个CCO帐户的Cisco.com。一旦验证，尝试手工下载Cisco IOS ？有K9特性组的软件包。

3. 检查是否有一个代理到位互联网限制流量的(除了7.2(1)的所有版本及以后)。如果从命令和控制端口的流量通过此代理，自动更新功能不运作。重新配置网络，以便命令和控制端口流量再没有过滤代理和测验。

4. 对于运行版本7.2或7.3软件的传感器，请保证一个或更多DNS服务器配置。这要求，以便传感器能解决www.cisco.com更新FQDN到互联网可路由IP地址。

5. 检查是否有任何内容过滤或流量整形应用程序或者设备在路径到互联网。若有，请配置排除为了允许命令和控制接口的IP地址访问互联网，不用限制。

6. 如果ICMP流量允许往互联网，请打开IPS传感器的CLI并且设法ping公网IP地址。

   此测验可以用于验证，如果必要路由和NAT规则(若被采用)正确地配置。如果ICMP测验成功，自动更新继续发生故障，请保证网络设备例如路由器和防火墙沿路径允许HTTPS和HTTP会话从IPS命令和控制接口IP。例如，如果命令和控制IP地址是10.1.1.1，在ASA防火墙的简单ACL条目能看起来象此示例：

   ```
   access-list INSIDE-TO-INTERNET extended permit tcp host 10.1.1.1 any eq www
   access-list INSIDE-TO-INTERNET extended permit tcp host 10.1.1.1 any eq https
   ```

7. CCO用户名不应该包含任何特殊字符，例如， @。 参考的Cisco Bug ID CSCsq30139欲知更多信息。

8. 当签名auto-update失败发生时，请使用下个表为了匹配相关的HTTP错误代码。

```
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
```

消息	含义
Error:自动更新例外：HTTP连接失败的[1,110]	认证失败。检查用户名和密码。
status=false自动更新例外：接收HTTP响应失败的[3,212]	对被计时的Auto Update服务器的请求。
Error:http错误反应：400	确保思科URL设置被默认。如果CCO ID比长度32个字符极大，请尝试不 CCO ID。这可以是在思科下载服务器的一个限制。
Error:自动更新例外：HTTP连接失败的[1,0]	网络问题被防止的下载或那里是一个潜在问题用下载服务器。