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

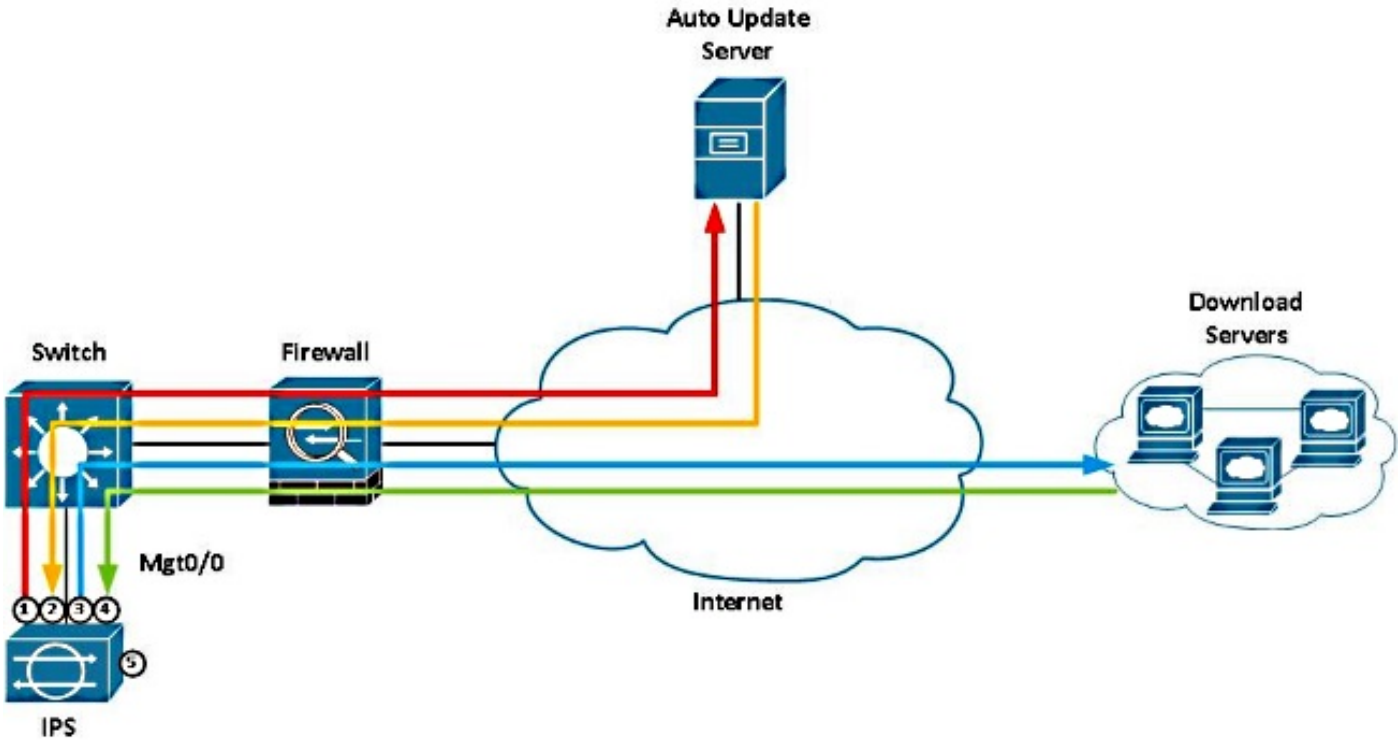
1. 使用HTTPS (TCP 443)和HTTP (TCP 80)， IPS的命令和控制接口要求直接访问到互联网。
2. 网络地址转换(NAT)和访问控制列表(ACL)在边缘设备例如路由器和防火墙需要配置为了允许IPS连接到互联网。
3. 从所有内容过滤器和网络流量成型机屏蔽命令和控制接口IP地址。
4. 在7.2(1) FIPS/CC被证实的版本的自动更新功能支持代理服务器。其他6.x和7.x软件版本不通过代理服务器支持自动更新此时。7.2(1)版本包括对默认安全壳SSH和HTTPS设置的一定数量的更改。 思科入侵防御系统的7.2(1)E4参考的版本注释，在您升级到7.2(1)前。

   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。**