Secure Client HostScan

AnyConnect 终端安全评估模块为 Secure Client提供标识主机上安装的操作系统、防恶意软件和防火墙软件的能力。HostScan 应用会收集此信息。终端安全状态评估要求在主机上安装 HostScan。

HostScan/Cisco Secure Firewall Posture 的前提条件

具有 Cisco Secure Firewall Posture/HostScan 的 Secure Client至少需要以下 ASA 组件：

- ASA 8.4
- ASDM 6.4

您必须安装 Cisco Secure Firewall Posture/HostScan 才能使用 SCEP 身份验证功能。

有关 Cisco Secure Firewall Posture/HostScan 安装支持的操作系统，请参阅支持的 VPN 平台，思科 ASA 系列。

HostScan 的许可

以下是 HostScan 的 Secure Client 许可要求：

- AnyConnect Apex
- AnyConnect 仅 VPN

HostScan 程序包

您可以将 HostScan 程序包作为独立的程序包加载至 ASA：**hostscan-version.pkg**。此文件包含 HostScan 软件，以及 HostScan 库和支持图表。

安装或升级 HostScan/Cisco Secure Firewall Posture

使用 ASA 的命令行界面，按照以下程序安装或升级 HostScan 或 Cisco Secure Firewall Posture 程序包并启用 HostScan。

开始之前

注释 如果您尝试从 HostScan 4.3.x 版或更低版本升级到 4.6.x 版或更高版本，由于您之前已制定的所有现有 AV/AS/FW DAP 策略和 LUA 脚本与 HostScan 4.6.x 版或更高版本不兼容，所以您将收到错误信息。

您必须完成一个一次性迁移程序来调整您的配置。此程序需要在保存此配置之前离开此对话框去迁移需要与 HostScan 4.4.x 兼容的配置。有关详细说明，请中止此程序并参阅《Secure Client HostScan 4.3.x 到 4.6.x 迁移指南》。简而言之，迁移过程涉及以下操作：导航到 ASDM DAP 策略页面检查并手动删除不兼容的 AV/AS/FW 属性，然后检查并重写 LUA 脚本。

- 登录 ASA 并进入全局配置模式。在全局配置模式下，ASA 将显示以下提示符：hostname(config)#
- 将 secure-firewall-posture-*version*-k9.pkg 上传到 ASA。如果您使用的是 HostScan 4.x 版本，则应上传 hostscan_*version*-k9.pkg 文件。

过程

步骤 1 进入 webvpn 配置模式。

示例：

```
hostname(config)# webvpn
```

步骤 2 打开 ASDM 并选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全状态（对于 Cisco Secure Firewall）(Posture [for Secure Firewall]) > 安全状态映像 (Posture Image)**。如果您使用的是 HostScan 4.x 版本，路径将为**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全桌面管理器 (Secure Desktop Manager) > 主机扫描映像 (Host Scan Image)**。

步骤 3 指定要指定为 HostScan/Cisco Secure Firewall Posture 映像的程序包的路径。您可以指定独立软件包或 Secure Client 软件包。

hostscan image *path*

示例：

如果您使用的是 HostScan 4.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081.pkg
```

如果您使用的是 Cisco Secure Firewall Posture 5.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

步骤 4 启用在上一步中指定的 HostScan/Cisco Secure Firewall Posture 映像。

示例：

```
ASAName(webvpn)#hostscan enable
```

步骤 5 将运行配置保存到闪存中。成功地将新配置保存到闪存中后，您将收到消息 [OK]。

示例：

```
hostname(webvpn)# write memory
```

步骤 6

启用或禁用 HostScan

这些命令使用 ASA 的命令行界面启用或禁用已安装的 HostScan 映像。

开始之前

登录 ASA 并进入全局配置模式。在全局配置模式下，ASA 将显示以下提示符：hostname(config)#

过程

步骤 1 进入 webvpn 配置模式。

示例：

webvpn

步骤 2 启用独立的 HostScan 映像（如果尚未将其从 ASA 中卸载）。

hostscan enable

步骤 3 为所有已安装的 HostScan 程序包禁用 HostScan。

注释
卸载已启用的 HostScan 映像之前，必须先使用以下命令禁用 HostScan。

no hostscan enable

查看 ASA 上启用的 HostScan/Cisco Secure Firewall Posture 版本

使用 ASA 的命令行界面，按照以下程序确定已启用的 HostScan/Cisco Secure Firewall Posture 版本。

开始之前

登录 ASA 并进入特权 EXEC 模式。在特权 EXEC 模式下，ASA 将显示以下提示符：hostname#

过程

显示 ASA 上启用的 HostScan/Cisco Secure Firewall Posture 版本

show webvpn hostscan

卸载 HostScan/Cisco Secure Firewall Posture

卸载 HostScan/Cisco Secure Firewall Posture 程序包会将其从 ASDM 界面的视图中移除并防止 ASA 部署该程序包，即使启用了它也是如此。卸载 HostScan/Cisco Secure Firewall Posture 不会从闪存驱动器中删除程序包。

开始之前

登录 ASA 并进入全局配置模式。在全局配置模式下，ASA 将显示以下提示符：hostname(config)#。

过程

步骤 1 进入 webvpn 配置模式。

webvpn

步骤 2 禁用要卸载的 HostScan/Cisco Secure Firewall Posture 映像。

no hostscanenable

步骤 3 指定要卸载的 HostScan/Cisco Secure Firewall Posture 映像的路径。可能已有一个独立程序包被指定为 HostScan/Cisco Secure Firewall Posture 程序包。

no hostscan image *path*

示例：

如果您使用的是 HostScan 4.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081-k9.pkg
```

如果您使用的是 Cisco Secure Firewall Posture 5.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg
```

步骤 4 将运行配置保存到闪存中。成功地将新配置保存到闪存中后，您将收到消息 [OK]。

write memory

将 Secure Client 功能模块分配到组策略

此程序将 Secure Client 功能模块与组策略关联。在 VPN 用户连接到 ASA 时，ASA 将下载这些 Secure Client 功能模块并将其安装到终端计算机上。

开始之前

登录 ASA 并进入全局配置模式。在全局配置模式下，ASA 将显示以下提示符：hostname(config)#

过程

步骤 1 为网络客户端访问添加内部组策略

group-policy *name* **internal**

示例：

```
hostname(config)# group-policy PostureModuleGroup internal
```

步骤 2 编辑新的组策略。输入该命令后，您会收到组策略配置模式的提示符：hostname(config-group-policy)#。

group-policy *name* **attributes**

示例：

```
hostname(config)# group-policy PostureModuleGroup attributes
```

步骤 3 进入组策略 webvpn 配置模式。输入该命令后，ASA 将返回以下提示符：hostname(config-group-webvpn)#

webvpn

步骤 4 配置组策略以便为组中的所有用户下载 Secure Client 功能模块。

anyconnect modules value *Cisco Secure Firewall* 模块 *Name*

anyconnect 模块命令的值可能包含下列一个或多个值。当指定多个模块时，请用逗号将这些值隔开。

值	Cisco Secure Firewall 模块/功能名称
dart	安全客户端 DART（诊断和报告工具）
vpngina	安全客户端 SBL（登录前开始）
posture	Cisco Secure Firewall Posture/HostScan
nam	安全客户端 网络访问管理器
none	单独使用可从组策略中删除所有 AnyConnect 模块。
profileMgmt	安全客户端 管理隧道 VPN

示例：

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

要删除某个模块，请重新发出命令，只指定要保留的模块值。例如，以下命令将删除 websecurity 模块：

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

步骤 5 将运行配置保存到闪存中。

成功地将新配置保存到闪存中后，您将收到消息 [OK]，并且 ASA 将返回以下提示符：
hostname(config-group-webvpn)#

write memory

HostScan/Cisco Secure Firewall Posture 相关文档

在 HostScan/Cisco Secure Firewall Posture 从终端计算机收集安全状态凭证后，您需要了解配置动态访问策略和使用 LUA 表达式来利用信息等主题。

以下文档详细介绍了这些主题：《思科自适应安全设备管理器配置指南》。另请参阅《思科安全客户端（包括 *AnyConnect*）管理员指南》，以获取有关 HostScan/Cisco Secure Firewall Posture 如何与 Secure Client配合工作的详细信息。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。