

为安全网络分析设备生成诊断包

目录

[简介](#)

[步骤](#)

[方法1.从管理器的Web用户界面\(UI\)](#)

[方法2.从每台设备的管理员UI](#)

[方法3.从每台设备的命令行界面\(CLI\)](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍收集安全网络分析(SNA)设备诊断包的不同步骤。

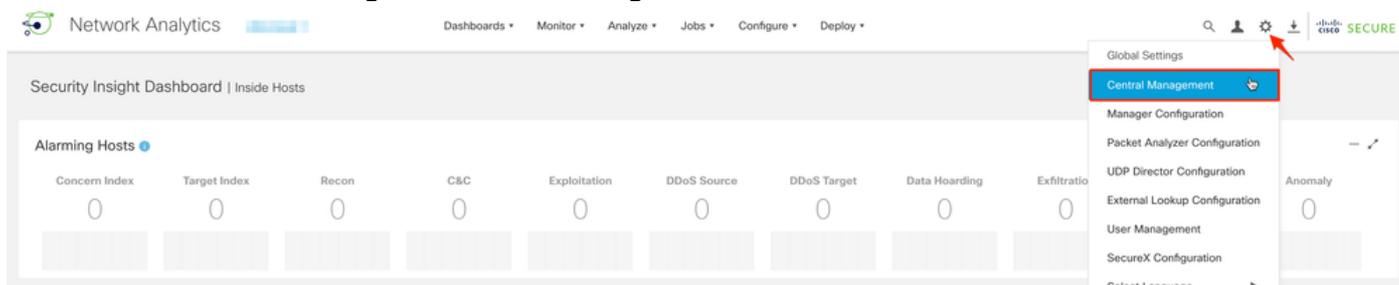
步骤

为SNA设备生成诊断包有三种主要方法。建议的方法是方法1。在Manager Web用户界面(UI)中，但在Manager的Web UI不可用时，其他两种方法是选项。

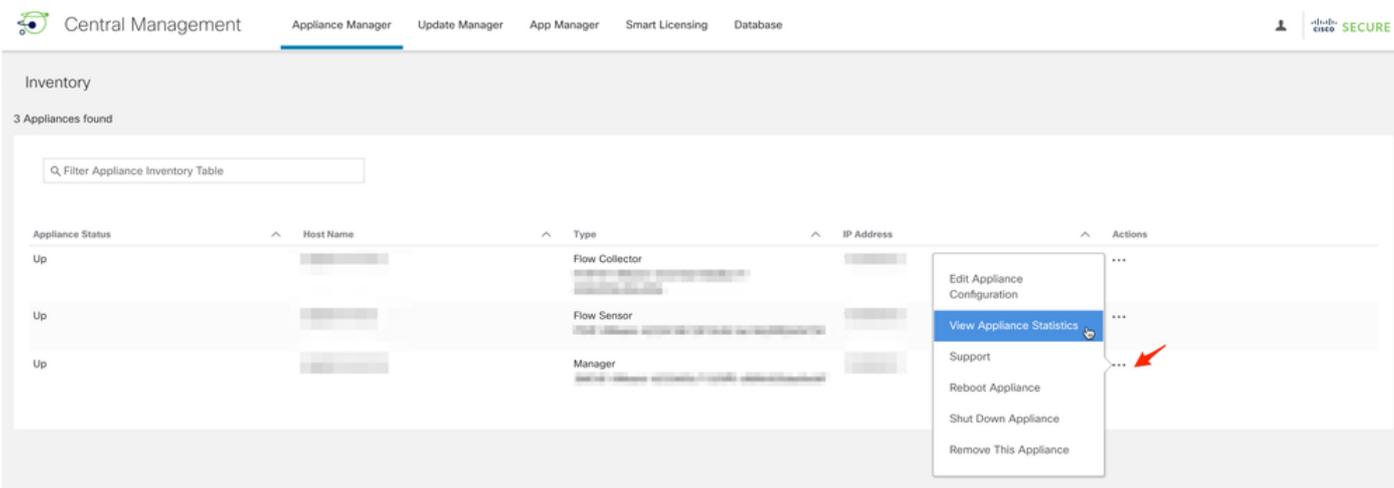
注意：如果Manager的Web UI不可用，并且您需要从Manager生成诊断包，请参阅方法3。从每台设备的命令行界面(CLI)。

方法1.从管理器的Web用户界面(UI)

1. 登录到Manager的Web UI。
2. 导航至**Global Settings > Central Management**。



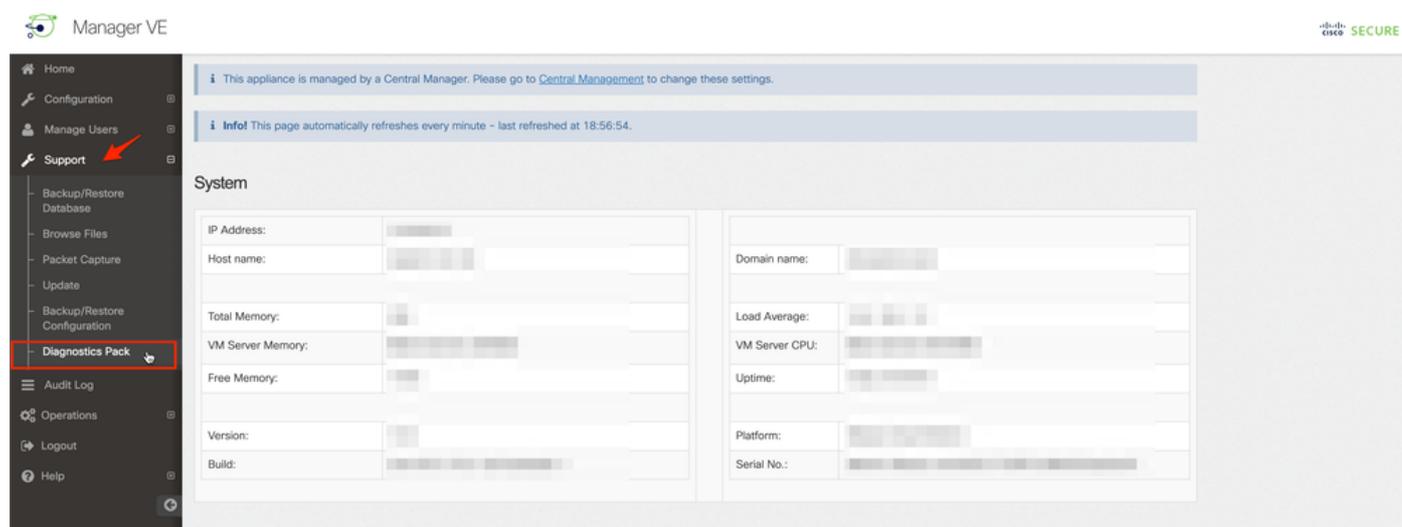
- 3.从列出的设备找到需要从其创建诊断包的设备，然后选择“操作 (省略号图标)”>“查看设备统计信息”。



4. 必须重定向到所选设备的管理员UI。

5. 使用管理员凭据登录设备管理员UI。

6. 从左侧的菜单导航至“支持”>“诊断包”。



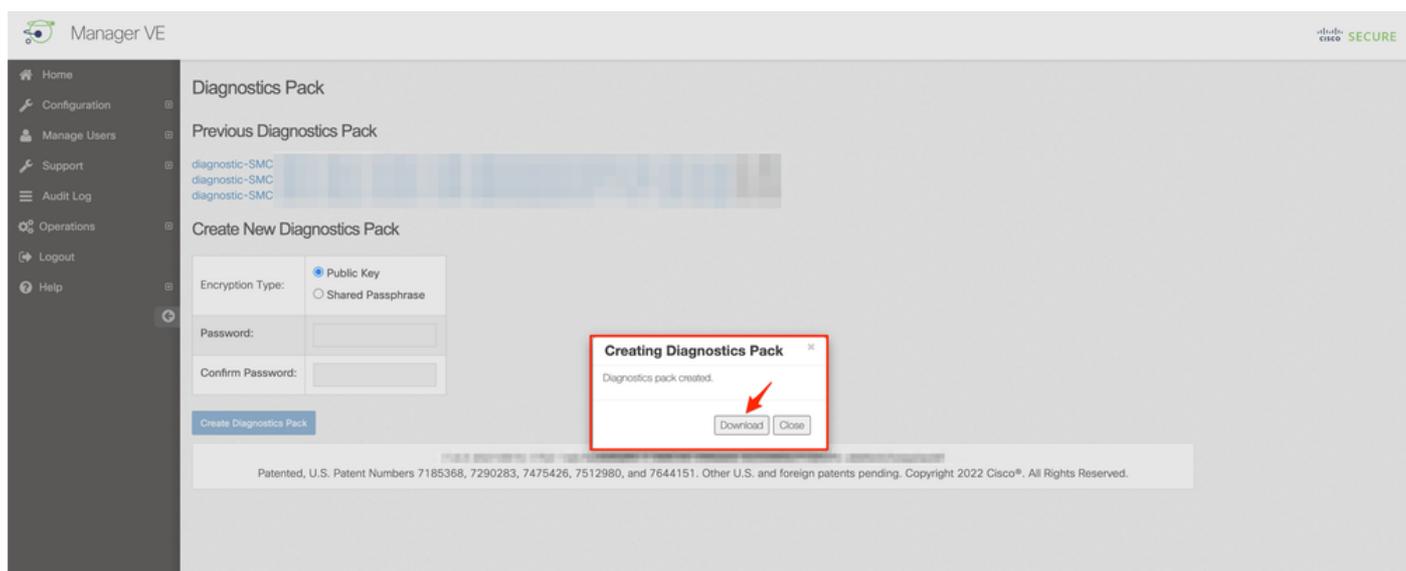
7. 进入“诊断包”页后，您需要选择默认的公钥加密，或提供共享密钥/密码以用于加密。

注意：如果选择使用自定义密钥/密码，则在将诊断包上传到支持案例管理器时，必须在文件说明中提供该密码。

8. 选择“创建诊断包”以生成设备的诊断包。



9.完成后，必须显示一个弹出框，其中包含“下载”按钮，以下载诊断包。



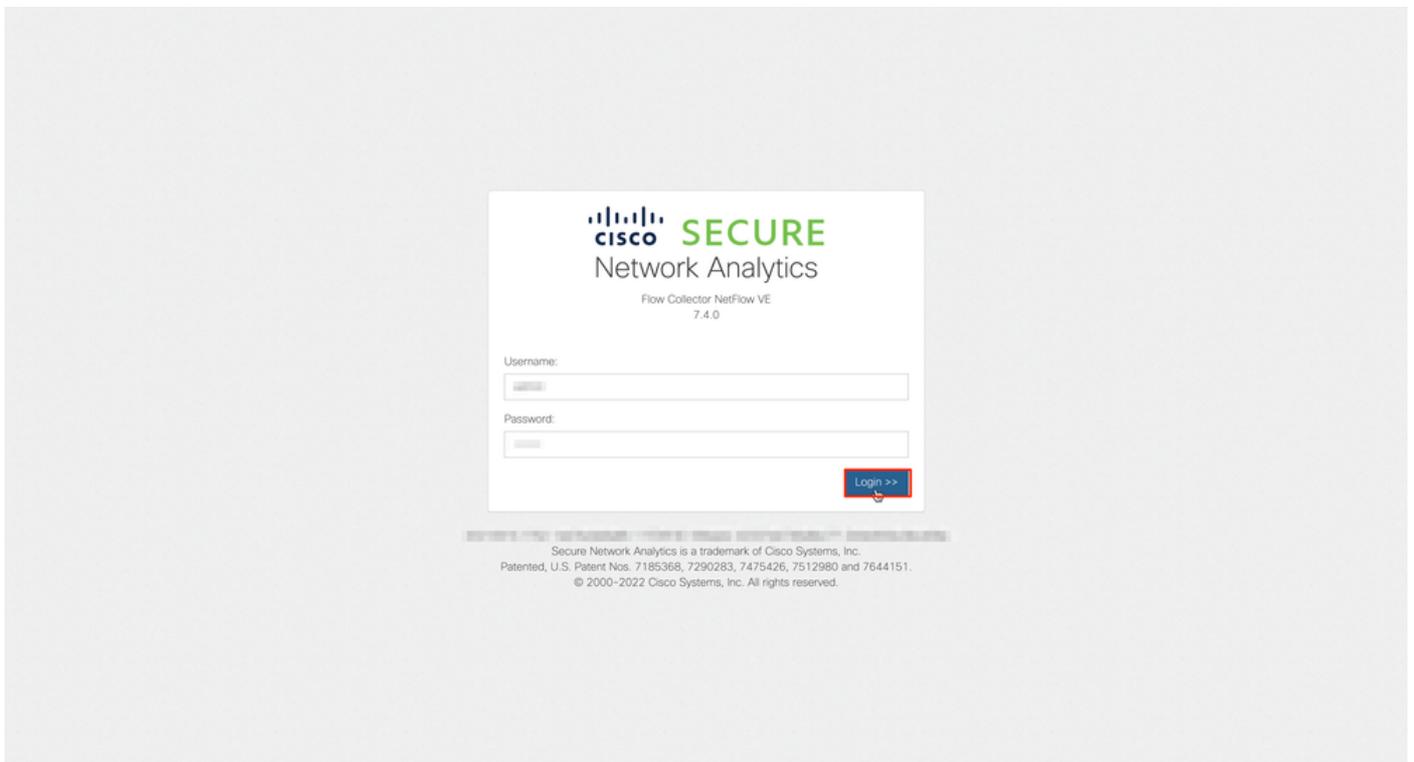
方法2.从每台设备的管理员UI

对于此方法，您必须通过安全超文本传输协议(HTTPS)访问要从中生成诊断包的设备。

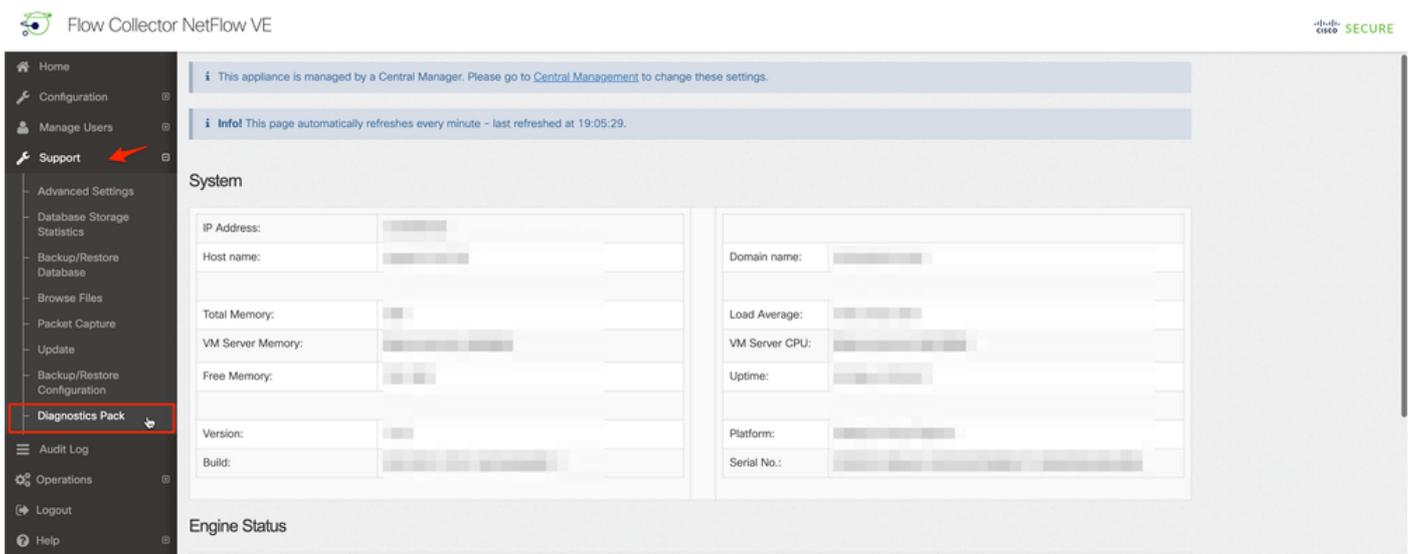
注意：要直接访问Manager的Admin UI，必须使用URL:https://<Manager_IP_address>/smc/index.html，否则您将重定向到Manager的Web UI。

例如，要使用此方法生成流量收集器的诊断包，必须执行以下步骤：

1. 从Web浏览器导航至https://<FC_IP_address>
2. 使用管理员凭证登录设备管理员UI。



3.从左侧的菜单导航至 支持>诊断包。



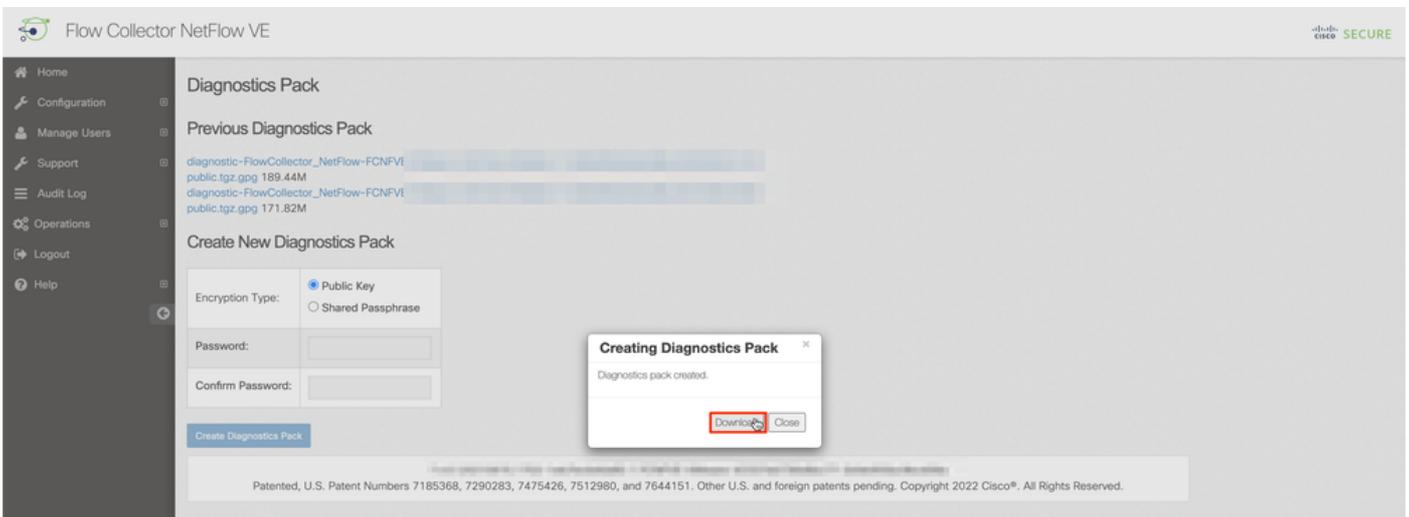
4.进入“诊断包”页后，您需要选择默认的公钥加密，或提供共享密钥/密码以用于加密。

注意：如果选择使用自定义密钥/口令，则在将诊断包上传到支持案例管理器时，必须在文件说明中提供该口令。

5.选择“创建诊断包”以生成设备的诊断包。



6.完成后，必须显示一个弹出框，其中包含“下载”按钮，以下载诊断包。



方法3.从每台设备的命令行界面(CLI)

有时无法使用前面介绍的方法生成设备的诊断包，但可以直接从设备的CLI生成。完成此任务的步骤如下：

1. 通过安全外壳协议(SSH)或直接通过控制台访问连接到所需的SNA设备。

注意：如果您需要从硬件设备收集诊断包，而无SSH访问，也可以使用思科集成管理控制器(CIMC)界面中的基于内核的虚拟机(KVM)控制台。

2. 使用根凭据登录。
3. 输入下一个命令之一（这取决于正在使用的SNA版本）：

SNA版本7.1.x到7.3.x

输入命令doDiagPack

SNA版本7.4.x

输入命令diagnostics start

4. 等待任务完成。
5. 任务完成后，诊断包文件将存储在/`lancope/var/admin/diagnostics/`目录中，名称方案为

```
"diagnostic-<Device_type>-<Device_ID>.<YYYYMMDD>.<HHMM>-* .tgz.gpg"
```

```
smc:/# doDiagPack
smc:/# ls -l /lancope/var/admin/diagnostics/
total 32740
-rw-r--r-- 1 root root 33522766 Feb 24 02:29 diagnostic-SMC-SMCVE-VMware-4
        -6                .20220224.0227-public.tgz.gpg
smc:/# █
```

6. 将生成的文件从设备复制到本地计算机或具有安全复制协议(SCP)或SSH文件传输协议(SFTP)客户端 (如WinSCP) 的文件服务器。诊断包位于/lancope/var/admin/diagnostics/目录中。

注：值得一提的是，SNA 7.4.0版引入了一项新功能，允许从SystemConfig菜单生成诊断包 (CLI登录并带**根凭证**> Enter **SystemConfig** >导航至**Recovery** > **Diagnostics Pack**)。

有关此方法的详细信息，请[参阅《安全网络分析系统配置指南7.4.x》](#)。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

有时，诊断包创建失败。最常见的症状是当您收到错误信息“**There war a error creating the diagnostics pack (创建诊断包时出错)**”时。单击“**Create Diagnostics Pack (创建诊断包)**”按钮后，“**No files are available (没有可用文件)**”。



要更正此行为，请按如下步骤操作：

1. 通过SSH使用根凭证登录到具有此行为的设备。
2. 运行**ls -l /lancope/var/database/dbs/hsqldb/admin/**命令以验证目录内容。
3. 确保备份子目录存在，并且其用户/组所有者为**tomcat**。

```
fcnf-cds:~# ls -l /lancope/var/database/dbs/hsqldb/admin/
total 20
-rw-r--r-- 1 tomcat tomcat 16 Apr 28 00:38 admin.lck
-rw-r--r-- 1 tomcat tomcat 0 Apr 27 17:20 admin.log
-rw-r--r-- 1 tomcat tomcat 84 Apr 27 17:17 admin.properties
-rw-r--r-- 1 tomcat tomcat 2995 Apr 27 17:17 admin.script
drwxr-xr-x 2 tomcat tomcat 4096 Apr 27 17:20 admin.tmp
drwxr-xr-x 2 tomcat tomcat 4096 Jun 7 2021 backup
```

如果备份子目录在/lancope/var/database/dbs/hsqldb/admin/path中不存在，则必须创建该子目录并分配正确的所有权。为此，请运行以下命令：

1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
2. chown tomcat /lancope/var/database/dbs/hsqldb/admin/backup
4. 运行ls -l /lancope/var/admin/命令以验证目录内容。
5. 确保备份和诊断子目录存在，并且其用户/组所有者是根。

```
fcnf-cds:~# ll /lancope/var/admin/
total 80
drwxrwxr-x 2 root root 4096 Apr 27 06:25 backups
drwxr-xr-x 2 root root 4096 Apr 7 21:39 cds
-rw-r--r-- 1 root root 0 Apr 6 22:10 clustered database
drwxrwxr-x 2 root root 4096 Sep 7 2021 diagnostics
-rw-r--r-- 1 root root 40 Apr 27 17:18 hwserial
-rw-r--r-- 1 root root 8 Apr 27 17:18 meminfo
-rw-r--r-- 1 root root 69 Apr 27 17:18 model
-rw-r--r-- 1 root root 23 Apr 27 17:18 platform
drwxr-xr-x 3 root root 4096 Sep 15 2021 plugins
-rw-rw-rw- 1 root root 2 Apr 27 18:13 previous_engine_startup_mode
-rw-r--r-- 1 root root 47 Apr 27 17:18 serial
drwxr-xr-x 2 root root 4096 Apr 7 21:22 ssh
drwxr-xr-x 2 root root 4096 Apr 8 02:51 system.d
-rw-rw---- 1 root swadmin 12756 Apr 8 02:56 system.xml
drwxrwxrwx 2 root root 4096 Apr 28 00:25 tmp
drwxr-xr-x 2 root root 4096 Sep 7 2021 update
drwxrwxr-x 4 root tomcat 4096 Apr 8 02:49 upgrade
-rw-r--r-- 1 root root 36 Apr 27 17:18 uuid
```

如果/lancope/var/admin/路径中不存在所述子目录中的一个或任何子目录，则必须创建它们并分配正确的所有权。为此，请运行以下命令：

1. mkdir /lancope/var/admin/backups
 2. mkdir /lancope/var/admin/diagnostics
- 检验完后，尝试再次生成SNA设备的诊断包。

相关信息

- 如需其他帮助，请联系思科技术支持中心(TAC)。需要有效的支持合同：[思科全球支持联系方式](#)
- [技术支持和文档 - Cisco Systems](#)