附录：与 macOS 11 (Big Sur) 相关的 AnyConnect 更改

您必须为 macOS 11 运行 AnyConnect 4.9.04xxx（或更高版本）。它利用 macOS 中可用的系统扩展框架，而之前使用的是现在已弃用的内核扩展框架。由于这一变化，管理员必须批准 AnyConnect 系统扩展，并要能够确认这些更新的正确操作。此外，如果遇到严重的系统扩展（或相关的操作系统框架）问题，作为最后的变通方法，您可以按照故障转移至 AnyConnect 内核扩展的步骤进行操作，但这仅出于此目的而安装且不会再默认使用

关于 AnyConnect 系统扩展

AnyConnect 在 macOS 11 上使用网络系统扩展，捆绑在名为 Cisco AnyConnect Socket Filter 的应用程序中。该应用程序会控制扩展的激活和停用，并安装在 /Applications/Cisco 下。

AnyConnect 扩展包含以下三个组件，可在 macOS 系统首选项 - 网络用户界面窗口中显示：

- DNS 代理
- 应用程序/透明代理
- 内容过滤器

AnyConnect 要求其系统扩展及其所有组件就能处于活动状态方可正常运行，这意味着上述组件全部安装到位，并在 macOS 网络用户界面的左窗格中显示为绿色（正在运行）。

批准 AnyConnect 系统扩展

macOS 11 要求最终用户进行扩展审批或无需最终用户审批的 MDM 审批，然后才能运行系统扩展。AnyConnect 系统扩展需要两个审批：

- 批准系统扩展加载/激活 ，第 2 页
- 使用 MDM 批准系统扩展 ，第 2 页

批准系统扩展加载/激活

按照操作系统提示或更明确的 AnyConnect 通知应用程序的说明，批准 AnyConnect 系统扩展及其内容过滤器组件。

过程

步骤 1 当您收到“系统扩展已阻止”(System Extension Blocked) 应用程序消息时，单击 AnyConnect 通知应用程序中的**打开首选项 (Open Preferences)** 按钮或**打开安全首选项 (Open Security Preferences)** 按钮。您还可以导航到“System Preferences”（系统首选项）应用程序并转到“Security&Privacy”（安全和隐私）窗口。

步骤 2 单击左下角的锁，然后提供请求的凭证以解锁并允许更改。

步骤 3 单击安全和隐私窗口中的**允许 (Allow)**，接受思科 AnyConnect 套接字过滤器。

当多个系统扩展需要审批时，按钮标记为“Details...”（详细信息...）。在这种情况下，单击**详细信息...(Details...)**，选中**思科 AnyConnect 套接字过滤器 (Cisco AnyConnect Socket Filter)** 复选框，单击**确定 (OK)**，然后批准需要“允许”(Allow) 的任何后续提示。

下一步做什么

当扩展程序的内容过滤器组件获得批准时，您将收到通知。

使用 MDM 批准系统扩展

使用管理配置文件具有以下设置的 SystemExtensions 负载来批准 AnyConnect 系统扩展而无需最终用户交互：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.anyconnect.macos.acsockext
系统扩展类型	NetworkExtension

使用以下 WebContentFilter 负载设置来批准扩展的内容过滤器组件：

特性	值
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	防火墙
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
PluginBundleID	com.cisco.anyconnect.macos.acsockext
VendorConfig	
UserDefinedName	思科 AnyConnect 内容过滤器

确认激活 AnyConnect 系统扩展

要确认 AnyConnect 系统扩展是否已获批准并激活，请运行 **systemextensionsctl list** 命令：

```
% systemextensionsctl list
1 extension(s)
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsockext
(4.9.03038/4.9.03038) Cisco AnyConnect Socket Filter Extension
[activated enabled]
```

您还可以检查系统首选项网络 UI 以确认所有三个 AnyConnect 扩展组件是否均已激活。

停用 AnyConnect 扩展

在 AnyConnect 卸载期间，系统会提示用户输入管理员凭证，以便批准停用系统扩展。

故障转移到内核扩展

AnyConnect仍在macOS11上安装其内核扩展；但如果出现严重的系统扩展（或相关操作系统框架）问题或在思科技术支持中心 (TAC) 的指示下，您应仅将其用作回退。在 macOS 11 上加载之前，内核扩展需要通过 MDM 审批。最终用户审批不再可供选择。

开始之前

仅将这些步骤用作最后的解决方法。

过程

步骤 1 使用管理配置文件的 *SystemPolicyKernelExtensions* 负载通过以下设置来批准 AnyConnect 内核扩展：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.kext.acsock

MDM 配置文件将进行安装。

步骤 2 运行以下会导致AnyConnect停用系统扩展并开始使用内核扩展的命令。系统将提示您输入管理员凭证。**% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && /Applications/Cisco/Cisco\ AnyConnect\ Socket\ Filter.app/Contents/MacOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plis**

步骤 3 运行以下命令以验证是否已加载内核扩展：**% kextstat | grep com.cisco.kext.acsock**

如果 AnyConnect 无法加载其内核扩展，请执行重新引导。

恢复到系统扩展

如果思科TAC确认修复了系统扩展问题（并消除了故障转移到内核扩展的需求），则可运行以下命令，指示 AnyConnect 切换回系统扩展：

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && sudo
 kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/anyconnect/acsock.cfg && sudo
launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

通过修复程序安装 AnyConnect 或 macOS 版本。

AnyConnect 系统和内核扩展批准的示例 MDM 配置文件

使用以下 MDM 配置文件来加载 AnyConnect 系统和内核扩展，包括系统扩展的内容过滤器组件。

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

      <dict>

      <key>PayloadContent</key>

      <array>

            <dict>

                  <key>AllowUserOverrides</key>

                  <true/>

                  <key>AllowedKernelExtensions</key>

                  <dict>

                        <key>DE8Y96K9QP</key>

                        <array>

                        <string>com.cisco.kext.acsock</string>

                        </array>

                  </dict>

                  <key>PayloadDescription</key>

                  <string></string>

                  <key>PayloadDisplayName</key>

                  <string>AnyConnect Kernel Extension</string>

                  <key>PayloadEnabled</key>

                  <true/>

                  <key>PayloadIdentifier</key>

                  <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>

                  <key>PayloadOrganization</key>

                  <string>Cisco Systems, Inc.</string>

                  <key>PayloadType</key>

                  <string>com.apple.syspolicy.kernel-extension-policy</string>

                  <key>PayloadUUID</key>

                  <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>

                  <key>PayloadVersion</key>

                  <integer>1</integer>
```

```
</dict>
<dict>
      <key>AllowUserOverrides</key>
      <true/>
      <key>AllowedSystemExtensions</key>
      <dict>
            <key>DE8Y96K9QP</key>
            <array>
            <string>com.cisco.anyconnect.macos.acsockext</string>
            </array>
      </dict>
      <key>PayloadDescription</key>
      <string></string>
      <key>PayloadDisplayName</key>
      <string>AnyConnect System Extension</string>
      <key>PayloadEnabled</key>
      <true/>
      <key>PayloadIdentifier</key>
      <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
      <key>PayloadOrganization</key>
      <string>Cisco Systems, Inc.</string>
      <key>PayloadType</key>
      <string>com.apple.system-extension-policy</string>
      <key>PayloadUUID</key>
      <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
</dict>
<dict>
      <key>Enabled</key>
      <true/>
      <key>AutoFilterEnabled</key>
```

```
                        <false/>
                        <key>FilterBrowsers</key>
                        <false/>
                        <key>FilterSockets</key>
                        <true/>
                        <key>FilterPackets</key>
                        <false/>
                        <key>FilterType</key>
                        <string>Plugin</string>
                        <key>FilterGrade</key>
                        <string>firewall</string>
                        <key>PayloadDescription</key>
                        <string></string>
                        <key>PayloadDisplayName</key>
                        <string>Cisco AnyConnect Content Filter</string>
                        <key>PayloadIdentifier</key>

<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
                        <key>PayloadType</key>
                        <string>com.apple.webcontent-filter</string>
                        <key>PayloadUUID</key>
                        <string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
                        <key>PayloadVersion</key>
                        <integer>1</integer>
                        <key>FilterDataProviderBundleIdentifier</key>
                        <string>com.cisco.anyconnect.macos.acsockext</string>
                        <key>FilterDataProviderDesignatedRequirement</key>
                        <string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9]
 /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
 leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string>
                        <key>PluginBundleID</key>
                        <string>com.cisco.anyconnect.macos.acsock</string>
```

```
                <key>UserDefinedName</key>
                <string>Cisco AnyConnect Content Filter</string>
            </dict>
        </array>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>Approved AnyConnect System and Kernel Extensions</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <true/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```