在本地策略中启用 FIPS

关于 FIPS、NGE 和 AnyConnect

AnyConnect 集成了思科通用加密模块 (C3M)。此思科 SSL 实施在其下一代加密 (NGE) 算法中，包含了符合联邦信息处理标准 (FIPS) 140-2 标准的加密模块和美国国家安全局 (NSA) 套件 B 加密。

NGE 引入新加密、身份验证、数字签名和密钥交换算法，以升级安全和性能需求。RFC 6379 定义了符合美国 FIPS 140-2 标准的套件 B 加密算法。

AnyConnect 组件根据前端、ASA 或 IOS 路由器的配置协商并使用 FIPS 标准加密。以下 AnyConnect 客户端模块支持 FIPS：

- AnyConnect 核心 VPN - 通过在用户计算机上的本地策略文件中使用 FIPS 模式参数，启用符合 FIPS 标准的 VPN 客户端。套件 B 加密适用于 TLS/DTLS 和 IKEv2/IPsec VPN 连接。有关详细信息和过程，请参阅为 AnyConnect 核心 VPN 客户端配置 FIPS。

  除 FIPS 模式以外，AnyConnect 本地策略文件 AnyConnectLocalPolicy.xml 还包含适用于本地客户端的其他安全设置。此文件并未通过 ASA 进行部署，且必须手动安装，或使用企业软件部署系统进行部署。有关使用此配置文件的详细信息，请参阅 AnyConnect 本地策略。

- AnyConnect 网络访问管理器 - 通过在 AnyConnectLocalPolicy.xml 文件中使用 FIPS 模式参数和在网络访问管理器配置文件中使用 FIPS 模式参数，启用符合 FIPS 标准的网络访问管理器。Windows 中支持用于网络访问管理器的 FIPS。有关详细信息和步骤，请参阅为网络访问管理器配置 FIPS。

AnyConnect 中的 FIPS 功能

功能	核心 VPN 模块	网络访问管理器模块
对称加密和完整性的 AES-GCM 支持。	用于 IKEv2 负载加密和身份验证的 128 位、192 位和 256 位密钥。 ESP 数据包加密和身份验证。	软件中有线流量加密的 802.1AE (MACsec) 的 128 位密钥 (Windows)。
哈希值算法的 SHA-2 支持，采用 256/384/512 位的 SHA。	IKEv2 负载身份验证和 ESP 数据包身份验证。（Windows 7 或更高版本和 macOS 10.7 或更高版本）。	能够在基于 TLS 的 EAP 方法中使用 SHA-2 证书。
密钥交换的 ECDH 支持。	组 19、20 和 21 IKEv2 密钥交换及 IKEv2 PFS。	能够在基于 TLS 的 EAP 方法中使用 ECDH (Windows)。
数字签名、不对称加密和身份验证的 ECDSA 支持，即 256 位、384 位、521 位椭圆曲线。	IKEv2 用户身份验证和服务器证书验证。	能够在基于 TLS 的 EAP 方法中使用 ECDSA 证书。
其他支持	IPsecV3 的所有必需加密算法（NULL 加密除外）。 IKEv2 的 Diffie-Hellman 组 14 和 24。 TLS/DTLS 和 IKEv2 的 4096 位密钥 RSA 证书。	不适用

[1] 在 Linux 中，对 ECDSA 仅支持 AnyConnect 文件存储。要向文件存储库添加证书，请参阅为 Mac 和 Linux 创建 PEM 证书存储库。

[2] IPsecV3 还规定必须支持扩展序列号 (ESN)，但 AnyConnect 不支持 ESN。

AnyConnect FIPS 要求

- 套件 B 加密适用于 TLS/DTLS 和 IKEv2/IPsec VPN 连接。
- 安全网关中需要 FIPS 和/或套件 B 支持。思科在 ASA 9.0 版及更高版本中提供套件 B 功能，在 ASA 8.4.1 版及更高版本中提供 FIPS 功能。
- ECDSA 证书要求：
  - 摘要强度必须大于或等于曲线强度。例如，EC-384 密钥必须使用 SHA2-384 或更高版本。
  - 支持的操作系统：Windows 7 或更高版本、macOS 10.7 或更高版本、Red Hat Enterprise Linux 6.x 或 6.4（64 位），以及 Ubuntu 12.4 和 12.10（64 位）。ECDSA 智能卡仅在 Windows 7（和更高版本）中受支持。

AnyConnect FIPS 的限制

在验证使用 SHA-2 签署的证书时，除了在基于 TLS 的 EAP 中，没有 EAP 方法支持 SHA-2。

AnyConnect FIPS 指南

- AnyConnect 客户端的 Statistics 面板（在 Transport Information 标题下）显示正在使用的密码名称。
- 由于 AES-GCM 是计算密集型的算法，因此使用这些算法时您可能会体验到整体数据速率降低。部分新 Intel 处理器包含专门引进以提升 AES-GCM 性能的特别说明。AnyConnect 会自动检测正在运行的处理器是否支持这些新指令。若支持，AnyConnect 将使用新指令，从而相对于那些没有特殊指令的处理器来说，可以显著提高 VPN 数据速率。请参阅 http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true 了解支持新指令的处理器列表。有关详细信息，请参阅 http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/。
- 组合模式加密算法（它在一次操作中同时执行加密和完整性验证）仅在具有硬件加密加速的 SMP ASA 网关（例如 5585 和 5515-X）上受支持。AES-GCM 是思科支持的组合模式加密算法。

  注释 IKEv2 策略既可以包含普通模式加密算法，也可以包含组合模式加密算法，但不能同时包含这两种类型。当组合模式算法配置在 IKEv2 策略中时，所有普通模式算法都被禁用，因此唯一有效的完整性算法为 NULL。

  IKEv2 IPsec 提议使用其他模型，可以在同一提议中同时指定普通模式和组合模式加密算法。对于这种用法，您需要为这两种算法都配置完整性算法，给 AES-GCM 加密算法配置的是非 NULL 完整性算法。
- 当 ASA 配置为对 SSL 和 IPsec 使用不同的服务器证书时，请使用受信任证书。如果使用具有不同 IPsec 和 SSL 证书的套件 B (ECDSA) 不受信任证书，则状态评估、WebLaunch 或下载程序可能发生故障。

避免因 AnyConnect FIPS 注册表更改导致的终端问题

为核心 AnyConnect 客户端启用 FIPS 会更改终端上的 Windows 注册表设置。终端的其他组件可能会检测到 AnyConnect 已启用 FIPS 并开始使用加密。例如，Microsoft 终端服务客户端远程桌面协议 (RDP) 将不工作，因为 RDP 要求服务器使用符合 FIPS 的加密。

为避免这些问题，您可以通过将参数 Use FIPS compliant algorithms for encryption, hashing, and signing 更改为 Disabled，在 Windows Local System Cryptography 设置中临时禁用 FIPS 加密。请注意重启终端设备将此设置改回已启用。

下表显示您应了解的 AnyConnect 执行的 Windows 注册表更改：

注册表项	更改
HKLM\System\CurrentControlSet\ Control\Lsa	FIPSAlgorithmPolicy 从 0 更改为 1。
HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	通过使用原始设置对 0x080 执行按位 OR 运算，SecureProtocols 设置更改为 TLSV1。
HKLM\Software\Policies\Microsoft\ Windows\CurrentVersion\Internet	通过使用原始设置对 0x080 执行按位 OR 运算，SecureProtocols 设置更改为 TLSV1。 这会为组策略设置 TLSv1。

为 AnyConnect 核心 VPN 客户端配置 FIPS

为 AnyConnect 核心 VPN 启用 FIPS

过程

步骤 1 在 AnyConnect 配置文件编辑器中打开或创建一个 VPN 本地策略配置文件。

步骤 2 选择 **FIPS Mode**。

步骤 3 保存此 VPN 本地策略配置文件。

我们建议您对此配置文件进行命名来表示已启用 FIPS。

在 Windows 安装期间启用 FIPS

对于 Windows 安装，您可以将 Cisco MST 文件应用于标准 MSI 安装文件，以便在 AnyConnect 本地策略中启用 FIPS。有关此 MST 文件的下载位置的信息，请参阅您收到的 FIPS 的许可信息。安装期间将生成已启用 FIPS 的 AnyConnect 本地策略文件。在运行此实用程序后，更新用户系统。

注释 此 MST 只启用 FIPS。它不会更改其他参数。要在 Windows 安装期间更改其他本地策略设置，请参阅在 MST 文件中启用本地策略参数。

为网络访问管理器配置 FIPS

网络访问管理器可配置为同时连接到 FIPS 和非 FIPS 网络，或者只连接到 FIPS 网络。

过程

步骤 1 为网络访问管理器启用 FIPS。

启用 FIPS 可允许网络访问管理器同时连接到 FIPS 和非 FIPS 网络。

步骤 2 如果需要，请参阅为网络访问管理器实施 FIPS 模式。

实施 FIPS 模式会将网络访问管理器连接仅限于 FIPS 网络。

为网络访问管理器启用 FIPS

过程

步骤 1 在 AnyConnect 本地策略中启用 FIPS 模式：

a) 在 AnyConnect 配置文件编辑器中打开或创建一个 VPN 本地策略配置文件。
b) 选择 **FIPS Mode**。
c) 保存此 VPN 本地策略配置文件。

我们建议您对此配置文件进行命名来表示已启用 FIPS。

步骤 2 在 AnyConnect 网络访问管理器客户端配置文件中启用 FIPS 模式：

a) 在 AnyConnect 配置文件编辑器中打开或创建一个网络访问管理器配置文件。
b) 选择 **Client Policy** 配置窗口。
c) 在 **Administrative Status** 部分下，为 **FIPS Mode** 选择 Enable。
d) 保存网络访问管理器配置文件。

我们建议您对此配置文件进行命名来表示已启用 FIPS。

为网络访问管理器实施 FIPS 模式

通过在网络访问管理器配置文件中限制允许的关联和加密模式以及身份验证方法，强制企业员工只连接到符合 FIPS 的网络。

必须首先为网络访问管理器启用 FIPS 以强制实施 FIPS 模式。

过程

步骤 1 在 AnyConnect 配置文件编辑器中打开网络访问管理器配置文件。

步骤 2 网络访问管理器 FIPS 合规性要求 FIPS 批准的 AES 加密模式，包括 WPA2 个人模式 (WPA2-PSK) 和 WPA2 企业模式 (802.1X)。

步骤 3 网络访问管理器 FIPS 支持 EAP 方法，包括 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST 和 LEAP。

步骤 4 保存网络访问管理器配置文件。

我们建议您将配置文件命名为指出只能进行 FIPS 连接。