Enable FIPS in the Local Policy

About FIPS, NGE, and AnyConnect

AnyConnect incorporates the Cisco Common Cryptographic Module (C3M). This Cisco SSL implementation includes Federal Information Processing Standard (FIPS) 140-2 compliant cryptography modules and National Security Agency (NSA) Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms.

NGE introduces new encryption, authentication, digital signatures, and key exchange algorithms for escalating security and performance requirements. RFC 6379 defines the Suite B cryptography algorithms conform to meet U.S. FIPS 140-2 standards.

AnyConnect components negotiate and use FIPS standard cryptography based on the configuration of the headend, an ASA or IOS router. The following AnyConnect client modules support FIPS:

- AnyConnect Core VPN—FIPS compliance for the VPN client is enabled using a FIPS-mode parameter in the local policy file on the user computer. Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections. See Configure FIPS for the AnyConnect Core VPN Client for details and procedures.

  The AnyConnect local policy file, AnyConnectLocalPolicy.xml, contains additional security settings beyond FIPS-mode that apply to the local client. It is not deployed by the ASA and must be installed manually, or deployed using an enterprise software deployment system. See The AnyConnect Local Policy for details on using this profile.

- AnyConnect Network Access Manager—FIPS compliance for the Network Access Manager is enabled using the FIPS-mode parameter in the AnyConnectLocalPolicy.xml file, and the FIPS-mode parameter in the Network Access Manager profile. FIPS for the Network Access Manager is supported on Windows. See Configure FIPS for the Network Access Manager for details and procedures.

FIPS Features in AnyConnect

Feature	Core VPN Module	Network Access Manager Module
AES-GCM support for symmetric encryption and integrity.	128-, 192-, and 256-bit keys for IKEv2 payload encryption and authentication. ESP packet encryption and authentication.	128-bit keys for 802.1AE (MACsec) for wired traffic encryption in software (Windows).
SHA-2 support for hashing, SHA with 256/384/512 bits.	IKEv2 payload authentication and ESP packet authentication. (Windows 7 or later and macOS 10.7 or later).	Ability to use certificates with SHA-2 in TLS-based EAP methods.
ECDH support for key exchange.	Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS.	Ability to use ECDH in TLS-based EAP methods (Windows).
ECDSA support for digital signature, asymmetric encryption, and authentication, 256-, 384-, 521-bit elliptic curves.	IKEv2 user authentication and server certificate verification.	Ability to use certificates with ECDSA in TLS-based EAP methods.
Additional support:	All required crypto algorithms for IPsecV3 except for NULL encryption. Diffie-Hellman Groups 14 and 24 for IKEv2. RSA certificates with 4096 bit keys for TLS/DTLS and IKEv2.	N/A

[1] On Linux, only the AnyConnect file store is supported for ECDSA. To add certificates to a file store, see Creating a PEM Certificate Store for macOS and Linux.

[2] IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but AnyConnect does not support ESN.

AnyConnect FIPS Requirements

- Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections.
- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the ASA version 9.0 and later, and FIPS capability on the ASA version 8.4.1 and later.
- ECDSA certificate requirements:
  - Must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
  - Are supported on Windows 7 or later, macOS 10.7 or later, Red Hat Enterprise Linux 6.x or 6.4 (64-bit), and Ubuntu 12.4 and 12.10 (64-bit). ECDSA smart cards are supported only on Windows 7 (and later).

Limitations of AnyConnect FIPS

No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.

Guidelines for AnyConnect FIPS

- The AnyConnect client's Statistics panel (under the Transport Information heading) shows the name of the cipher being used.
- Because AES-GCM is computationally intensive algorithms, you may experience a lower overall data rate when using these algorithms. Some new Intel processors contain special instructions specifically introduced to improve the performance of AES-GCM. AnyConnect automatically detects whether the processor on which it is running supports these new instructions. If so, AnyConnect uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special instructions. See http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=truefor a list of processors that support the new instructions. For more information, see http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/.
- Combined-mode encryption algorithms, where both encryption and integrity verifications are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X). AES-GCM is the combined-mode encryption algorithm that Cisco supports.

Note An IKEv2 policy can include either a normal- or a combined-mode encryption algorithm, but not both types. When a combined-mode algorithm is configured in the IKEv2 policy, all normal-mode algorithms are disabled, so the only valid integrity algorithm is NULL.

The IKEv2 IPsec proposals use a different model and can specify both normal- and combined-mode encryption algorithms in the same proposal. With this usage, you are required to configure integrity algorithms for both, which leaves a non-NULL integrity algorithm configured with AES-GCM encryption.

- When the ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture Assessment, WebLaunch, or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.

Avoiding Endpoint Problems from AnyConnect FIPS Registry Changes

Enabling FIPS for the core AnyConnect client changes Windows registry settings on the endpoint. Other components of the endpoint may detect that AnyConnect has enabled FIPS and started using cryptography. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work, because RDP requires that servers use FIPS compliant cryptography.

To avoid these problems, you can temporarily disable FIPS encryption in the Windows Local System Cryptography settings by changing the parameter Use FIPS compliant algorithms for encryption, hashing, and signing to Disabled. Be aware that rebooting the endpoint device changes this setting back to enabled.

Registry Key	Changes
HKLM\System\CurrentControlSet\ Control\Lsa	FIPSAlgorithmPolicy changed from 0 to 1.
HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting.
HKLM\Software\Policies\Microsoft\ Windows\CurrentVersion\Internet	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting. This sets TLSv1 for a group policy.

Configure FIPS for the AnyConnect Core VPN Client

Enable FIPS for the AnyConnect Core VPN

Procedure

Step 1 Open or create a VPN Local Policy profile in the AnyConnect Profile Editor.

Step 2 Select **FIPS Mode**.

Step 3 Save the VPN Local Policy profile.

We recommend that you name the profile to indicate that FIPS is enabled.

Enable FIPS During Windows Installation

For Windows installations, you can apply a Cisco MST file to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. For information about where you can download this MST file, see the licensing information you received for FIPS. The installation generates an AnyConnect Local Policy file with FIPS enabled. Update the user’s system after running this utility.

Note This MST only enables FIPS. It does not change other parameters. To change other local policy settings during Windows installation, see Enable Local Policy Parameters in an MST File.

Configure FIPS for the Network Access Manager

The Network Access Manager can be configured to connect to both FIPS and non-FIPS networks simultaneously, or to FIPS networks only.

Procedure

Step 1 Enable FIPS for the Network Access Manager.

Enabling FIPS allows the Network Access Manager to connect to both FIPS and non-FIPS networks.

Step 2 If desired, Enforce FIPS Mode for the Network Access Manager.

Enforcing FIPS mode restricts the Network Access Manager connections to FIPS networks only.

Enable FIPS for the Network Access Manager

Procedure

Enable FIPS mode in the AnyConnect Network Access Manager client profile:

a) Open or create a Network Access Manager profile in the AnyConnect Profile Editor.
b) Select the **Client Policy** configuration window.
c) Under the **Administrative Status** section select **Enable** for **FIPS Mode**.
d) Save the Network Access Manager profile as configuration.xml.

Enforce FIPS Mode for the Network Access Manager

Force enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods in the Network Access Manager profile.

You must first Enable FIPS for the Network Access Manager to enforce FIPS mode.

Procedure

Step 1 Open your Network Access Manager profile in the AnyConnect Profile Editor.

Step 2 Network Access Manager FIPS compliance requires FIPS-approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X).

Step 3 The Network Access Manager FIPS support includes EAP methods EAP-TLS, EAP-TTLS, PEAP, EAP-FAST and LEAP.

Step 4 Save the Network Access Manager profile as configuration.xml.