FIPS 140-2 FIPS Mode

Introduction:

Check Point appliances implement a FIPS mode developed to define an operational mode compliant with the requirements of:

- The NIST CMVP FIPS 140-2 standard
- Common Criteria Protection Profile compliance as recognized by NIAP-CCEVS

FIPS Compliance Configuration

Enabling FIPS mode on the Security Gateway

1. Enables use of cpu-jitter for generating entropy and /dev/random for the entropy pool (manual configuration described in section "Outside of FIPS Mode" below). Enables enforcement of self-tests that verify authenticity of the signed cryptographic module libraries and their integrity during startup and verifies that the functional correctness on the operation of the cryptographic algorithms. In case where a test fails, the boot cycle will fail to complete and the system will not become operational. When not in FIPS mode the boot tests will execute and on failure the result is written to a system log file and the system will become operational. Check Point updates/patches are signed as part of the build process. When in FIPS mode these are validated before they can be installed. The administrator can validate the authenticity of libraries or executables using the filesign command.
2. FIPS mode disables SSH, Web UI, the remote installation daemon cprid_d and removes support for SSLv3 from SIC (i.e. only TLS is supported). When in FIPS mode access to the fw, fwm, and vpn command line utilities are removed. FIPS mode disables SecurXL and AES-NI. CPRID is disabled as are the QOS blade and the monitoring blade. We have investigated CPRID and this uses SIC to communicate so can be enabled.

Configuration:

3. The gateway must be managed by a SMART-1 Management Server.
4. Strict compliance with the SP 800-56A rev3 standard will come into force at the end of 2020. Compliance reduces the ciphers allowed for key agreement within IPsec, TLS and therefore SIC.
    - For TLS this is automatically configured on the Security Gateway when enabling FIPS mode for the Check Point Cryptographic Library V1.1 as the only allowed ECDHE based cyphers are: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA:TLS ECDHE_RSA_WITH_AES_128_CBC_SHA256:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.
    - For IPsec the allowed groups defined in the Security Policy are 14, 19 and 20.
5. When running in an approved mode the administrator is only allowed to use FIPS approved algorithms shown in the table of "Cryptographic Algorithms" section of the FIPS 140-2 Security Policy that are written at the end of this document.

General Configuration (not related to FIPS mode):

6. P-256, P-384 and P-521 are fully supported through use of an external CA.
    - The Gateway is able to generate keys, CSRs and receive a signed certificate.

Outside of FIPS mode:

7. Entropy can be configured by the administrator so that it is generated using cpu-jitter and that it is drawn from /dev/random (rather than /dev/urandom) In standard mode two steps are required to achieve the same:

- On Gateway, run “chkconfig --add jitterentropy_rngd_init” and “chkconfig --level 2345 jitterentropy_rngd_init on”
- Add an environment variable by editing $CPDIR/tmp/.CPprofile.sh and adding the following line:
    - USE_ONLY_GOOD_ENTROPY=1 ; export USE_ONLY_GOOD_ENTROPY
    - Then reboot.

8. Native SSH can be configured so that it only supports approved FIPS algorithms by editing the ssh_config and sshd_config files in /etc/ssh directory
   aes128-ctr,aes192-ctr,aes256-ctr
   And hmac-sha1
   SSH has not been validated as part of the FIPS certification so is not approved for operation.
9. SNMPv3 is allowed in FIPS, but it is not considered approved, even where AES is used, as the key is too small to provide adequate security. SNMPv3 with AES is thus considered to provide obfuscation and not encryption.
10. The SIC policy may be configured from the expert cpshell command as follows:
    - cp $CPDIR/conf/sic_policy.conf $CPDIR/conf/sic_policy.conf.bak
    - cp $CPDIR/conf/fips_sic_policy.conf $CPDIR/conf/sic_policy.conf

Cryptographic Algorithms

The following table provides details of the approved algorithms that are included within the module at R80.30:

Algorithm Type	Algorithm	CAVP Certificate Number	Notes
Symmetric key	AES	#3418	AES with 128-bit or 256-bit keys using CBC and GCM[1] modes. The modes and sizes are validated for both encryption and decryption.
Asymmetric Key	RSA	#1750	Key generation (2048–bit keys). Signature generation (2048-bit/3072-bit with either SHA-256, SHA-384 or SHA-512). Signature verification. (1024-bit/2048-bit signature verification with either SHA-1, SHA-256, SHA-384 or SHA-512).
	ECDSA	#685	Supports P-256, P-384, and P-521 curves. FIPS186-4: PKG: CURVES(P-256 P-384 P-521 Testing Candidates) PKV: CURVES(P-256 P-384 P-521) SigGen: CURVES(P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512) SigVer: CURVES(P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512))
Hashing	SHS	#2824	SHA-1[2] (disallowed for signature generation), SHA-256, SHA-384, SHA-512.

[1] The module complies with SP 800-52 and is compatible with the specified versions of TLS in Section 4 of RFC 5288.
The module complies with RFC 6071 and that an IKEv2 protocol (RFC 7296) shall be used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.
[2] SHA-1 for non-digital signature applications:
SHA-1 is not allowed for digital signature generation. For all other hash function applications, the use of SHA-1 is acceptable. The other applications include HMAC, Key Derivation Functions (KDFs), and hash-only plications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140-2]).

Algorithm Type	Algorithm	CAVP Certificate Number	Notes
Message Authentication Code	HMAC	#2176	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384.
Random number generator	Hash DRBG	#823	Hash DRBG with SHA-256 and a seed length of 440 bits in accordance with SP800-90A.
Key Agreement	KAS-SSC	Vendor Affirmed	SP 800-56A rev3 for IPsec and TLS.

The following table lists the key derivation functions (and their associated CVL certificate numbers) implemented by the module.

Approved KDF	CAVP CVL Certificate Number
Transport Layer Security (TLS) v1.0/1.1, v1.2 (SP 800-135)	#514
Internet Key Exchange (IKE) v1 and v2 (SP 800-135)	#514

Approved Key Derivation Functions

