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 Compliant Versions:

1. Check Point Cryptographic Module V1.1 is validated with certificate 4264 with R80.30 as the tested platform.
2. Check Point Cryptographic Module V1.1 was tested using R80.30, R80.30SP and CloudGuard and used Network on Enterprise Gateways as tested platforms.
3. R80.40, R81 and R81.10 are claimed in the official Security Policy with a vendor assertion as compliant as allowed in FIPS 140-2 Implementation Guidance IG G.5
4. Appliances not tested by FIPS were tested as part of the NIAP R81 Common Criteria (CC) certification where they also needed to comply with NIST requirements by having validated entropy and CAVP certificates. The Common Criteria tested in a CC and FIPS compliant configuration, which is provided in the Administrative Guidance. The R81 CC Security Target that provides a list of certified platforms and the Administrative Guidance can be found at https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11235
5. The R81 Common Criteria certification is complementary to FIPS, Protection Profile compliance to:
    a. Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (cPP_ND_v2.2e) herein referenced as NDcPP22e
    b. PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, 1.1, 18 June 2020 (MOD_VPNGW_v1.1) herein referenced as VPNGW11
    c. PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e, 25 June 2020 (MOD_cPP_FW_v1.4e) herein referenced as STFFW14e
6. The cryptographic claims are compliant with the NSA Commercial Software for Classified (CSfC), which allows product use for protecting classified NSS data. R81 is listed on the CSfC https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/

©2022 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

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 is 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, WebUI, 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 AES-NI, CPRID the QOS blade and the monitoring blade. Note: CPRID may be enabled as it uses SIC. It was disabled for historical reasons. WebUI is confirmed to use the certified cryptographic library, but is not claimed as a service.

Configuration:

3. The gateway is certified in a "sandwich" configuration with a separate Management Server.
4. The gateway is compliant with SP 800-56A rev3 standard come into force at the end of 2020. Compliance reduces the ciphers allowed for key agreement within IPsec, TLS and therefore SIC.
5. In FIPS mode TLS is automatically configured on the Security Gateway when enabling FIPS mode and only allows these ECDHE based cyphers:
   - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA:TLSECDHE_RSA_WITH_AES_128_CBC_SHA256:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.
   - IPsec allowed groups are 14, 19 and 20.
6. 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):

7. 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:

8. FIPS compliant 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:
   - On Gateway, run "chkconfig --add jitterentropy_rngd_init" and "chkconfig --level 2345 jitterentropy_rngd_init on"

©2022 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

- 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.

9. 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.
10. 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.
11. 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.con

Cryptographic Algorithms The following table provides details of the approved algorithms that are included within the module:

ALGORITHM TYPE	ALGORITHM	CAVP CERTIFICATE NUMBER	NOTES
Symmetric key	AES	#3418	AES with 128-bit or 256-bit keys using CBC and GCM[123] 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
	ECDSA	#685	verification with either SHA-1,

[1] The module complies with SP 800-52 Rev2 and is compatible with the specified versions of TLS in Section 4 of RFC 5288.
The module complies with RFC 6071 and RFC 4106 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. The module also complies with RFC 5282 for authenticated encryption of the encrypted payload of the IKEv2 protocol.
[2] Once the counter portion of the IV reaches its maximum value of 2^32-1, the module aborts the session.
[3] In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

©2022 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Algorithm Type	Algorithm	CAVP Certificate Number	Notes
			SHA-256, SHA-384 or SHA-512). 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[4], SHA-256, SHA-384, SHA-512.
Message Authentication Code	HMAC	#2176	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512.
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-ECC-SSC	Vendor Affirmed	SP 800-56A rev3 for IPsec and TLS.

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-ECC-SSC	Vendor Affirmed	SP 800-56A rev3 for IPsec and TLS.

Figure 1 Approved Algorithms

[4] 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 applications (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]).

©2022 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

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 Rev1)	#514
Internet Key Exchange (IKE) v1 and v2 (SP 800-135 Rev1)	#514

Figure 2 Approved Key Derivation Functions

For each of these approved Key Derivation Functions the module supports or uses the corresponding protocol. These protocols have not been reviewed or tested by the CAVP or CMVP as testing such protocols is not within the scope of CMVP or CAVP activities.

©2022 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals