Table of Contents

AlgoPedia > Data Collection

Failure to Connect to Check Point via OPSEC due to Lack of OPSEC Certificate

Error message

Error: 15/12/04-08:48:18 [/usr/share/fa/php/commands/checkpoint_firewall_handler.cmd.php:557] GetOpsecCertification() - <user> - Failed to fetch OPSEC certificate, rc=4

In the /home/afa/.fa-history log file, the following error appears:

Error: Failed to establish both authenticated and non-authenticated LEA connection to 1.2.3.4
Info: Authenticated LEA connection in debug mode results:
[3402 4150212304]@algosec[4 Dec 8:48:06] opsec_auth_client_connected: SIC Error for lea: Could not retrieve CRL.
ERROR: SIC ERROR 325 - SIC Error for lea: Could not retrieve CRL.
[3402 4150212304]@algosec[4 Dec 8:48:08] opsec_auth_client_connected: SIC Error for lea: Could not retrieve CRL.
ERROR: SIC ERROR 325 - SIC Error for lea: Could not retrieve CRL.
Info: get_opsec_certificate: Restoring old certificate
moving opsec_cpmi.conf_old to opsec_cpmi.conf
Info: [3334] 15/12/04-08:48:12 fa_server - Executed: /usr/share/fa/bin/get_opsec_certificate "m_1_2_3_4" "1.2.3.4" "algosec" "******" "18190" "18184" "sslca" "sslca" "0" "test_lea"
ExitCode=512
Error: [3334] 15/12/04-08:48:12 fa_server - Failed to get OPSEC certificate.

Problem

Adding a Check Point device via OPSEC fails due to the failure to fetch the OPSEC certificate (SIC error 325).

Cause

Check Point management is configured to use SHA-256, and not SHA-1. This hash is not supported in Check Point's OPSEC API, which is used by AlgoSec, as well as by all third-party platforms integrating with Check Point via OPSEC.

SHA-256 was introduced in Check Point R71 and will become the default hash algorithm from Version R80 and later versions.

Solution

Configure the Check Point management to use SHA-1, instead of SHA-256.

This allows the creation of a certificate and the establishment of trust with the AlgoSec server. After establishing the trust, the Check Point configuration can be changed back to SHA-256. The certificate should continue to be valid.

Alternatively, configure AFA to connect to the Check Point management via SSH and not OPSEC.
For more information, refer to Check Point SK-103840.

6.11 and above:

Navigate to the CLI, and type the following parameter:
" CKP_OPSEC_SHA2=yes ".