F5 BIG-IP 16.1.3.1 (2024.1088) and BIG-IP 17.1.0.1 (2024.1266) Administrative Guide Document (AGD) Appendix for CSfC Transport Layer Security (TLS) Protected Server Use Case

Installation and Upgrade

When downloading system images from the F5 Downloads site, be sure to download the 3072-bit public key and the ISO signature files associated with that key.

SSL Profiles

In the 17.1.0.1 AGD section 2.3.11.1, and 16.1.3.1 AGD section 2.3.10.1, SSL Profiles, the second to last paragraph should be amended to say, “When configuring SSL profiles, only use 3072-bit or higher RSA key sizes, or ECDSA curve p-384” to ensure that cryptographic keys used are 3072-bit or higher.

TLS Versions and Cipher Suites

AGD Section 5.1 Allowed Ciphersuites for TLS and SSH: TLS, the TLS table includes the cipher suite row, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. The column “Control Plane Server” for this row should say “TLS1.2” instead of “N/A”. This cipher suite and only CSfC-approved cipher suites should be configured following instructions in this MyF5 article: https://my.f5.com/manage/s/article/K01770517.

Certificate Validation

The AGD section 3.8 Certificate Validation should be amended to include support for RFC 8603. The first sentence should say, “The TOE supports validation of X.509 digital certificates using a certificate revocation list (CRL) as specified in [RFC 5280] Section 5 and RFC 8603.”

Session Resumption

The AGD section 3.10 Session Resumption should be revised to disable session resumption. The following should be added:

Session resumption must be disabled. This can be achieved by disabling session tickets and SSL session caching. Two options need to be configured for this.

First, set the clientssl profile ‘cache size’ to 0.

```
tmsh modify ltm profile client-ssl  <client_ssl_name> cache-size 0
```

Then disable session tickets if they are not already disabled.

```
tmsh modify ltm profile client-ssl  <client_ssl_name> session-ticket disabled
```