Is the PNC channel between DMZ Gateway® and EFT FIPS certified?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, 7.4.x and later

QUESTION

Is the PNC channel between DMZ Gateway® and EFT FIPS certified?

ANSWER

For the FIPS certified cryptographic module implementation in EFT version 7.2.9 and 7.3.6 (and subsequent releases), Globalscape is using version 2.0.10 of the OpenSSL FIPS Object Module. The NIST FIPS certificate is #1747, which can be found in the NIST Computer Resource Center. When EFT is configured to use SSL, the EFT administrator can specify which protocols and ciphers to use. The DMZ Gateway uses the same protocols, ciphers, and certificate that EFT uses. Therefore, if EFT is configured with FIPS-certified protocols and ciphers, the PNC channel between EFT and DMZ Gateway is encrypted using the same FIPS-certified libraries. certificates used outside of EFT that are not FIPS compliant may cause the connection to not be FIPS complaint.

The version of OpenSSL EFT is using, 1.0.2t, also includes 1.0.2t-fips; therefore, if this is enabled on EFT and a certificate is created by EFT this would fall under the same FIPS 140-2 technology that could be used in DMZ. Certificates created outside of EFT that are not FIPS compliant may cause the connection to not be FIPS compliant.

EFT administrators can use whatever certificate they want for this, or use a certificate created by EFT. EFT supports the following ciphers for FIPS:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Is the PNC channel between DMZ Gateway® and EFT FIPS certified?

TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS 1.1 and 1.2 support is provided.

In DMZ Gateway, open gwconfig.xml in the root of the install folder. If the SecurePNCEnabled setting is set to true, then it also acts like a “require SSL” setting in that only secure peer notification channels will be allowed. In other words, whether or not a channel is to be secured is enforced by the server and not solely dictated by the client.

Is the PNC channel between DMZ Gateway® and EFT FIPS certified?

<PNCTrustStorePath>C:\devel\certs\truststore.jks</PNCTrustStorePath>

<PNCStorePassphrase>GSBEvsavuSo9cA6OO18fS5B+ubI+zdoDBYTzMoA3vtDQiiA65hLnVLdRAwyIZStqezbp

<PNCProtocols>TLSv1.2,TLSv1.1,TLSv1</PNCProtocols>

<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_

See also "Secure PNC Settings" in the online help for your version of EFT or DMZ Gateway.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11516/Is-the-PNC-channel-between-D...