

Cipher support on NetScaler VPX FIPS and MPX FIPS certified appliances

The following appliances are NetScaler FIPS appliances:

- MPX 8900 FIPS
- MPX 9100 FIPS
- MPX 9200 FIPS
- MPX 15000-50G FIPS
- VPX FIPS

The following table lists the support for different ciphers on SSL entities, such as virtual server, services, and internal services.

Cipher Suite Name	Hex Code	Wireshark Cipher Suite Name
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS1.2-ECDHE-ECDSA-AES256-SHA384	0xc024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS1.2-ECDHE-ECDSA-AES128-SHA256	0xc023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	0xc02c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	0xc02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS1.3-AES256-GCM-SHA384	0x1302	TLS_AES_256_GCM_SH A384
TLS1.3-AES128-GCM-SHA256	0x1301	TLS_AES_128_GCM_SH A256