Supernova测试仪支持进行IPsec/SSL VPN隧道测试。

其中，IPsec VPN阶段1算法包括6种加密算法、6种摘要算法、10个DH组；阶段2算法包括6种加密算法、6种摘要算法、8个DH组；

SSL VPN支持SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3、国密v1.1共6种SSL版本。

其中：SSLv3支持的加密套件：4种；

TLSv1.0支持的加密套件：8种；

TLSv1.1支持的加密套件：8种；

TLSv1.2支持的加密套件：27种；

TLSv1.3支持的加密套件：3种；

国密v1.1支持的加密套件：4种。

类别	支持加密算法
IPsec VPN	阶段1算法 加密算法：sm4cbc、aes-128、aes-192、aes-256、des、3des，共6种； 摘要算法：sm3、sha1、sha2-256、sha2-384、sha2-512、md5，共6种； DH组：group1、group2、group5、group14、group15、group16、group17、group18、group22、group23，共10个。
	阶段2算法 加密算法：sm4cbc、aes-128、aes-192、aes-256、des、3des，共6种； 摘要算法：sm3、sha1、sha2-256、sha2-384、sha2-512、md5，共5种； DH组：group1、group2、group5、group14、group15、group16、group17、group18，共8个。
	SSLv3支持的加密套件：AES128-SHA、AES256-SHA、DHE-RSA-AES128-SHA、DHE-RSA-AES256-SHA，共4种；
	TLSv1.0支持的加密套件：AES128-SHA、AES256-SHA、DHE-RSA-AES128-SHA、ECDHE-RSA-AES128-SHA、ECDHE-ECDSA-AES128-SHA、DHE-RSA-AES256-SHA、ECDHE-RSA-AES256-SHA、ECDHE-ECDSA-AES256-SHA，共8种；
	TLSv1.1支持的加密套件：AES128-SHA、AES256-SHA、DHE-RSA-AES128-SHA、ECDHE-RSA-AES128-SHA、ECDHE-ECDSA-AES128-SHA、DHE-RSA-AES256-SHA、ECDHE-RSA-AES256-SHA、ECDHE-ECDSA-AES256-SHA，共8种；

SSL VPN	TLSv1.2支持的加密套件：AES128-SHA、AES256-SHA、AES128-SHA256、AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-RSA-AES128-SHA、ECDHE-RSA-AES128-SHA、ECDHE-ECDSA-AES128-SHA、DHE-RSA-AES256-SHA、ECDHE-RSA-AES256-SHA、ECDHE-ECDSA-AES256-SHA、DHE-RSA-AES128-SHA256、ECDHE-RSA-AES128-SHA256、ECDHE-ECDSA-AES128-SHA256、DHE-RSA-AES256-SHA256、ECDHE-RSA-AES256-SHA384、ECDHE-ECDSA-AES256-SHA384、DHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES128-GCM-SHA256、DHE-RSA-CHACHA20-POLY1305、ECDHE-RSA-CHACHA20-POLY1305、ECDHE-ECDSA-CHACHA20-POLY1305、DHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES256-GCM-SHA384，共27种；
	TLSv1.3支持的加密套件：TLS_AES_128_GCM_SHA256、TLS_CHACHA20_POLY1305_SHA256、TLS_AES_256_GCM_SHA384，共3种；
	国密v1.1支持的加密套件：ECC-SM4-SM3、ECDHE-SM4-SM3、RSA-SM4-SM3、RSA-SM4-SHA1，共4种。