Supernova测试仪功能列表

用例功能	功能分类	功能介绍
HTTP	HTTP每秒新建会话	获取受测设备新建HTTP会话的最快速率，每个虚拟用户建立一条TCP连接，执行一次完整的HTTP的事务(发送请求和接收回应)，最后关闭连接。再新建TCP连接并包含一次完整的HTTP会话。
	HTTP最大并发会话	获取受测设备支持的最大HTTP并发连接数，每个虚拟用户建立大量的TCP连接，每条连接循环完成HTTP事务(发送请求和接收回应)，最后关闭TCP连接。
	HTTP最大请求会话	获取受测设备处理HTTP请求的最快速率，每个虚拟用户建立一条TCP连接，循环完成多个HTTP事务(发送请求和接收回应)，最后关闭TCP连接。
	HTTP最大吞吐速率	获取受测设备的最大HTTP吞吐量，每个虚拟用户建立一条TCP连接，循环完成HTTP事务(发送请求和接收回应)，最后关闭连接。
	HTTP事务	与Jmeter的HTTP测试功能类似，可以自动解析Cookie并保持会话状态，在完成HTTP事务测试的过程中，可以使用变量和断言。
HTTPS （支持国密、RSA)	HTTPS每秒新建会话	获取受测设备新建HTTPS会话的最快速率，每个虚拟用户建立一条TCP连接，并进行SSL握手连接，完成HTTPS事务(发送请求和接收回应)，最后关闭连接。再新建TCP连接并包含一次完整的HTTPS会话。
	HTTPS最大并发会话	获取受测设备支持的最大HTTPS并发连接数，每个虚拟用户建立大量TCP连接，每条连接循环完成HTTPS事务(发送请求和接收回应)，最后关闭TCP连接。
	HTTPS最大请求会话	获取受测设备处理HTTPS请求的最快速率，每个虚拟用户建立一条TCP连接，并进行SSL握手连接，循环完成多个HTTPS事务(发送请求和接收回应)，最后关闭TCP连接。
	HTTPS最大吞吐速率	获取受测设备的最大HTTPS吞吐量，每个虚拟用户建立一条TCP连接，循环完成HTTPS事务(发送请求和接收回应)，最后关闭连接。
	HTTPS事务	与Jmeter的HTTPS测试功能类似，可以自动解析Cookie并保持会话状态，在完成HTTPS事务测试的过程中，可以使用变量和断言。
HTTP2	HTTP2每秒新建会话	获取受测设备基于TLS/SSL的HTTP2新建会话的最快速率，每个虚拟用户建立一条TCP连接，进行SSL握手，完成HTTP2事务(发送请求和接收回应)，最后关闭连接。再新建TCP连接并包含一次完整的HTTP2S会话。
	HTTP2最大吞吐速率	获取受测设备基于TLS/SSL的HTTP2的最大吞吐量，每个虚拟用户建立一条TCP连接，循环完成HTTP2事务(发送请求和接收回应)，最后关闭连接。
RTSP/RTP/RTCP	RTSP视频播放新建	获取受测设备播放流媒体的最快新建速率，每个虚拟用户建立RTSP/RTP/RTCP连接，控制终端与服务器之间的媒体传输事务，最后关闭所有连接，循环往复。
	RTSP视频播放质量	获取受测设备播放流媒体的清晰度，并根据RFC4445，算出MDI和相关数据，与配置的MDI清晰度范围进行比较，统计数量。每个虚拟用户建立RTSP/RTP/RTCP连接，控制终端与服务器之间的媒体传输事务，最后关闭TCP连接。
	RTSP视频播放并发	获取受测设备处理流媒体的并发量，并根据RFC4445，算出MDI和相关数据。每个虚拟用户建立RTSP/RTP/RTCP连接，控制终端与服务器之间的媒体传输事务，最后关闭TCP连接。虚拟用户数量就是并发的媒体播放数量。
	RTSP视频播放吞吐	获取受测设备处理流媒体的吞吐量，并根据RFC4445，算出MDI和相关数据。每个虚拟用户建立RTSP/RTP/RTCP连接，控制终端与服务器之间的媒体传输事务，最后关闭TCP连接。提高虚拟用户数量、播放码率就会提高吞吐率。
	音频播放质量	获取受测设备处理音频流媒体的并发量及语音质量，并根据RFC4445，计算Mos值等相关数据。每个虚拟用户循环播放音频流媒体，虚拟用户数量就是并发的音频播放用户数量。
	IPsec VPN新建	获取受测设备新建IPSec隧道的最快值，每个虚拟用户循环建立一条远程访问的IPSec隧道，通过隧道执行完整的HTTP事务(TCP连接，HTTP请求和回应，关闭TCP连接)，并终止隧道。

IPSec VPN	**IPsec VPN并发**	获取受测设备支持的最大IPSec并发隧道数，建立大量的IPSec(IKE)隧道连接，并通过它循环执行完整的HTTP事务，最后终止隧道。
	IPsec VPN吞吐	获取受测设备IPSec隧道的吞吐值，建立IPSec（IKE）隧道连接，并通过它循环执行完整的HTTP事务，最后终止隧道。
SSL VPN	**SSL VPN并发**	获取受测设备支持的最大SSLVPN并发隧道数，大量的SSLVPN隧道连接，并通过它循环执行完整的HTTP事务，最后终止隧道。
通用协议	**通用协议新建**	获取受测设备的处理通用协议的性能，每个虚拟用户建立一条TCP连接，使用默认TCP通用协议流模板，发送和接受TCP载荷，然后关闭连接，再新建TCP连接，依据模板发送TCP协议流，循环往复。
	通用协议吞吐	获取受测设备的处理通用协议的性能，每个虚拟用户建立一条TCP连接，使用默认TCP通用协议流模板，发送和接受TCP载荷，然后关闭连接，再新建TCP连接，依据模板发送TCP协议流，循环往复。
	通用协议并发	获取受测设备的处理通用协议的性能，每个虚拟用户建立一条TCP连接，使用默认TCP通用协议流模板，发送和接受TCP载荷，然后关闭连接，再新建TCP连接，依据模板发送TCP协议流，循环往复。
TCP	**TCP每秒新建会话**	获取受测设备新建TCP连接的最快速率，每个虚拟用户新建TCP连接后，关闭TCP连接。
	TCP最大吞吐速率	获取受测设备的最大TCP吞吐量，每个虚拟用户建立一条TCP连接，每条连接都可以双向发送和接收数据，最后关闭TCP连接。
	SMTP邮件发送速率	获取受测设备处理邮件发送的最快速率，每个虚拟用户循环建立TCP连接，通过SMTP发送一封电子邮件，并关闭TCP连接。
	POP3邮件接收速率	获取受测设备处理邮件接收的最快速率，每个虚拟用户循环建立TCP连接，通过POP3接收一封电子邮件，并关闭TCP连接。
	IMAP邮件接收速率	获取受测设备处理邮件接收的最快速率，每个虚拟用户循环建立TCP连接，通过IMAP接收一封电子邮件，并关闭TCP连接。
	FTP文件传输速率	获取受测设备处理FTP文件传输的最快速率，每个虚拟用户循环建立TCP连接，通过FTP协议传输一个文件，然后关闭TCP连接。
	LDAP每秒执行搜索	获取受测设备处理LDAP的能力，每个虚拟用户建立TCP连接，用LDAP协议查找节点信息，最后关闭连接。
	PostgreSql速率	获取受测设备处理SQL语句发送的最快速率，每个虚拟用户循环建立TCP连接，发送一些SQL语句，并关闭TCP连。
	MySQL速率	获取受测设备处理SQL语句发送的最快速率，每个虚拟用户循环建立TCP连接，发送一些SQL语句，并关闭TCP连接。
	SSH交互会话	获取受测设备处理SSH交互会话的最快速率，每个虚拟用户循环建立TCP连接，模拟SSH交互会话，并关闭TCP连接。
	RDP能力	获取受测设备处理RDP的能力，每个虚拟用户循环建立RDP连接，发送fastpath格式事件，并关闭TCP连接。
	Telnet速率	获取受测设备处理Telnet登录和运行命令的最快速率，每个虚拟用户循环建立TCP连接，通过Telnet协议登录服务器，并执行pwd命令，最后关闭TCP连接。
	RTMP	获取受测设备实时数据通信的网络协议，主要用来在Flash/AIR平台和支持RTMP协议的流媒体/交互服务器之间进行音视频和数据通信。
	UDP最大吞吐速率	获取受测设备的最快报文转发率和最大吞吐量，每个虚拟用户以最快速度发送UDP帧，通过发送和接收的差值，确定受测设备的报文转发率和吞吐量。
	UDP载荷转发速率	获取受测设备处理特定载荷的最快转发率和最大吞吐量，每个虚拟用户发送具有特定载荷的UDP帧，通过发送和接收的差值，确定受测设备的报文转发率和吞吐量。
	NTP每秒时间同步	获取受测设备处理NTP请求的成功率和时延，每个虚拟用户向NTP服务器发送NTP查询并接收回应，计算请求的成功率和时延。
	DNS每秒请求回应	获取受测设备处理DNS请求的成功率和时延，每个虚拟用户发送DNS请求并接收回应，计算请求的成功率和时延。

UDP	**HANDLE请求速率**	Handle协议在工业物联网中，使用数字对象标识符(Digital Object Identifier DOI) 对联网对象进行标识。测试模拟Handle协议的客户端，使用DOI查询对象的信息，并进行统计。
	TFTP文件传输速率	获取受测设备处理TFTP文件传输的最快速率，每个虚拟用户发送TFTP请求，并接收回应。
	RADIUS认证速率	获取受测设备处理RADIUS认证的最快速率，每个虚拟用户发送RADIUS请求，并接收回应。
	5G_MCI命令响应	MCI(Media Control Interface),Supernova测试仪与5G测试仪，共同组成5G测试方案。此用例接收从5G测试仪发出的业务开始、暂停、恢复、停止等命令，进行流量仿真和业务控制。
	SIP请求会话	SIP（Session Initiation Protocol）会话初始协议是一种信令协议，是VoIP技术的IETF标准，测试仪模拟多个虚拟用户，获取受测设备处理多媒体会话的能力。
DHCP	**DHCPv4**	获取受测设备处理DHCP请求的时延，V4:向DHCP服务器发送DHCP请求并测量时延
	DHCPv6	获取受测设备处理DHCP请求的时延，V6:通过DHCPv6无状态模式，发送NS和RA请求并测量时延。
IPoE	**IPoE吞吐**	每个虚拟用户，在客户端接口上，虚拟出一个子接口，发送DHCP请求获取IP地址后，再广播ARP报文获取网关MAC地址，然后每个子接口都发送UDP报文，并在服务器端口上接收UDP报文
	IPoE认证	每个虚拟用户，在客户端接口上虚拟出一个子接口，发送DHCP请求获取IP地址后，再广播ARP报文获取网关MAC地址，然后每个子接口都与认证服务器进行交互，发送认证请求，仿真从DHCP动态获取IP地址到认证登录的交互过程。
DNS协议	**DNS_over_UDP**	通过UDP协议发送DNS查询请求，并获取受测设备处理请求的成功率和时延，每个虚拟用户通过UDP协议发送DNS请求并接收回应，计算请求的成功率和时延。
	DNS_over_HTTPS	通过HTTPS发送DNS查询请求，并获取受测设备处理请求的成功率和时延，每个虚拟用户通过HTTPS发送DNS请求并接收回应，计算请求的成功率和时延。
工控协议	**Modbus新建**	客户端模拟MODBUS的主站，服务器模拟MODBUS的从站，主站新建tcp连接，向从站发送一系列指令，从站接收到指令执行相应动作并回复状态，关闭tcp连接；再次新建tcp连接重复发送指令，完成MODBUS新建仿真测试。
	Modbus吞吐	获取受测设备的最大Modbus吞吐量，每个虚拟用户建立一条Modbus连接，循环完成Modbus指令交互，最后关闭连接。
	Modbus并发	获取受测设备支持的最大Modbus并发连接数，每个虚拟用户建立大量的Modbus连接，每条连接循环完成Modbus指令交互，最后关闭连接。
	OPCUA新建	根据关联的OPCUA协议流模板，每个虚拟用户建立一个OPCUA连接，依据OPCUA载荷模板的载荷内容，进行报文发送和接收，以及数据统计，关闭连接；再次新建连接，进行报文的发送和接收，完成OPCUA新建仿真测试。
	OPCUA吞吐	获取受测设备的最大OPCUA吞吐量，每个虚拟用户建立一跳OPCUA连接，循环完成此用例中关联的OPCUA协议流模板中的报文交互，最后关闭连接。
	OPCUA并发	获取受测设备支持的最大OPCUA并发连接数，每个虚拟用户建立大量的OPCUA连接，每条连接循环完成此用例关联的OPCUA协议流模板中的报文交互，最后关闭连接。
	IEC61850_MMS新建	此用例根据关联的IEC61850_MMS协议流模板，每个虚拟用户建立一个IEC61850_MMS连接，依据IEC61850_MMS载荷模板的载荷内容，进行报文发送和接收，以及数据统计，关闭连接；再次新建连接，进行报文的发送和接收，完成IEC61850_MMS新建仿真测试。
	IEC61850_MMS吞吐	获取受测设备的最大IEC61850_MMS吞吐量，每个虚拟用户建立一条IEC61850_MMS连接，循环完成此用例中关联的IEC61850_MMS协议流模板中的报文交互，最后关闭连接。
	IEC61850_MMS并发	获取受测设备支持的最大IEC61850_MMS并发连接数，每个虚拟用户建立大量的IEC61850_MMS连接，每条连接循环完成此用例关联的IEC61850_MMS协议流模板中的报文交互，最后关闭连接。

	S7COMM新建	此用例根据关联的S7COMM协议流模板，每个虚拟用户建立一个S7COMM连接，依据S7COMM载荷模板的载荷内容，进行报文发送和接收，以及数据统计，关闭连接；再次新建连接，进行报文的发送和接收，完成S7COMM新建仿真测试。
	S7COMM吞吐	获取受测设备的最大S7COMM吞吐量，每个虚拟用户建立一条S7COMM连接，循环完成此用例中关联的S7COMM协议流模板中的报文交互，最后关闭连接。
	S7COMM并发	获取受测设备支持的最大S7COMM并发连接数，每个虚拟用户建立大量的S7COMM连接，每条连接循环完成此用例关联的S7COMM协议流模板中的报文交互，最后关闭连接。
	Dnp3	客户端模拟Dnp3的主站，服务器模拟Dnp3的子站，主站向子站发送指令，子站接收并回复状态，完成协议模拟并进行各种统计。
组播协议	**IGMP组播处理**	IGMP(Internet Group Management Protocol)互联网组管理协议是TCP/IP 协议族中负责IP组播成员管理的协议，用来在IP主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。支持 v1/v2/v3 三个版本。
	MLD组播处理	组播侦听者发现协议MLD（Multicast Listener Discovery）是负责IPv6组播成员管理的协议，用来在IPv6成员主机和与其直接相邻的组播路由器之间建立和维护组播组成员关系。MLD通过在成员主机和组播路由器之间交互MLD报文实现组成员管理功能，MLD报文封装在IPv6报文中。
动态路由协议	**RIPv1v2**	在测试仪端口上模拟支持RIPv1v2协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	RIPng	RIPng是RIPv2的扩展，用来支持IPv6。在测试仪端口上模拟支持RIPng协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	OSPFv2	在测试仪端口上模拟支持OSPFv2协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	OSPFv3	在测试仪端口上模拟支持OSPFv3协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	BGPv4	在测试仪端口上模拟支持BGPv4协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	BGP4+	在测试仪端口上模拟支持BGP4+协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
	ISISv4	在测试仪端口上模拟支持ISISv4协议的路由器（Emulated Router），向受测路由设备通告内部的路由信息（Simulated Router），并在每条路由上发送和接收UDP流量，判断路由是否连通，获取受测设备处理路由信息和选路连通的能力。
MPLS协议	**LDP_SESSION**	MPLS LDP是多协议标签交换MPLS的一种控制协议，根据MPLS LDP协议，创建网络主要节点的会话Session，生成标签交换路径LSP。
	MPLS_IP_VPN	MPLS IP VPN是通过MPLS技术和MP-BGP技术结合，通过两层标签传输实现的IP层VPN。
RFC2544基准测试	**RFC2544吞吐**	依据RFC2544规定的吞吐量测试标准，获取受测设备的吞吐量。吞吐量是指受测设备在不丢包的情况下，所能转发的最大数据流量。
	RFC2544时延	依据RFC2544规定的时延测试标准，获取受测设备的时延。时延是网络设备接收、处理、转发报文的时间。
	RFC2544丢包率	依据RFC2544规定的丢包率测试标准，获取受测设备的丢包率。丢包率是指在一定的负载下，由于缺乏资源而未被转发的报文占应当转发的报文数的百分比。
	RFC2544背靠背	根据RFC2544规定的背靠背测试标准，获取受测设备的缓存能力。背靠背值产生过程为：以最大速率发送一定长度的数据包，并不断改变一次发送的数据包数目，直到受测设备能转发所有包，这个包数就是受测设备的背靠背值。

RFC2889基准测试	**RFC2889地址缓存容量测试**	确定局域网交换设备的地址缓存容量。以指定速率从客户端网口向DUT网口，发送源MAC地址不同而目的MAC地址相同的帧，然后测试帧被DUT转发至服务端网口，监听端口监听泛洪帧或者转发错误帧，通过二分法的应用可确定DUT在无泛洪和无错误转发情况下，正确学习并转发的最大地址数。
	RFC2889MAC地址学习速率	获取局域网交换设备的MAC地址学习最快速率，以高速率从客户端网口向DUT发送源MAC地址不同而目的地址相同的帧。源地址个数即DUT的地址缓存容量。然后测试帧被DUT转发至服务端网口。监听端口监听泛洪帧或者转发错误帧。通过二分法的应用可确定DUT在无泛洪和无错误转发情况下的最大学习速率（单位为帧每秒）。
RFC3918基准测试	**混合吞吐量测试**	依据RFC3918规定的混合吞吐量测试标准，获取受测设备在同时转发组播和单播流量的时候的吞吐量。吞吐量是指受测设备在不丢包的情况下，所能转发的最大数据流量。
流量重放	**快速流量重放**	检测受测设备处理特定网络报文流的状态，该测试可以重放特定格式的通过Tcpdump或者Wireshark捕获的pcap文件（具体的格式要求可以通过点击“对象->PCAP对象->增加->增加”，在“PCAP文件上传设置”页面中查看），检测受测设备的处理状态。
	攻击流量重放	感知受测设备的入侵检测和防御能力，该测试重放已知的网络攻击数据流，通过检查重放报文的完整性，确定受测设备的入侵检测和防御能力。系统预置攻击报文数量10248个，涉及HTTP、HTTPS、UDP、SMTP、Microsoft、MySQL、Oracle、DNS等攻击类型。
	工控协议重放	检测受测设备对各种工控数据流的处理状态，内置多种工控协议。该测试通过重放各种工控协议pcap文件来检测受测设备的处理状态。
IPv6一致性检测	**IPv6一致性检测**	为了保证各种 IPv6 实现版本与 IPv6 协议标准一致及相互之间能够安全、可靠地相互通信，需要对 IPv6 协议进行 IPv6 Ready Logo Phase-2 检测和认证，当前包含 5 个大项共 319 个小项。
数据流量模型	**数据流量模型**	检验受测设备处理多种网络流量的状况，把各种网络流量混合，模拟真实的网络传输，并检验受测设备的状态，当前可以混合 32 种类型的用例。
	封装Stream	根据流模板配置，按照限速的比例封装各种报文，在流量发送时，可以依据报文各个字段的跳变策略，对报文内容进行自动更改，每个端口最多可以构建256条流。
安全检测评估	**系统漏洞扫描**	扫描、评估和管理目标主机上的漏洞。请到官网-支持与下载 页面，下载最新的漏洞库。 系统预置漏洞库漏洞数量99369个，其中包括高危漏洞40150个、中等漏洞49359个、低危漏洞9859个。
	Web攻击靶场	扫描指定Web服务的信息，并运用10 种编码技术，进行SQL/XSS注入和WebShell等 14 种Web攻击，既支持攻击模式（只模拟客户端攻击服务器），也支持靶场模式（客户端攻击，服务端运行靶场应用如bWAPP/DVWA等），运行靶场模式请到官网下载靶场组件。
	网络服务检测	主机发现，检测主机上开放的端口，检测相应端口提供的服务，检测操作系统，硬件地址，以及软件版本等等，当前共包含 10 种扫描配置。
	IPv4报文分片攻击	检测受测设备抵御分片攻击的能力，每个虚拟用户以最快速度发送分片攻击报文，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 13 种IPv4报文分片攻击：TEARDROP_UDP_FLOOD、TEARDROP_TCP_FLOOD、NEWTEAR_FLOOD、FAWX_FLOOD、BONK_FLOOD、NESTA_FLOOD、ROSE_TCP_FLOOD、ROSE_UDP_FLOOD、LARGE_OFFSET_FRAG_FLOOD、PING_OF_DEATH_FLOOD、JOLT_FLOOD、LARGE_NUMBER_OF_FRAG_FLOOD、IDENTICAL_REPEAT_OF_FRAG_FLOOD
	ICMPv4单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送ICMPv4单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 14 种ICMPv4单包攻击：ICMP_FLOOD、ICMP_IP_FRAG_FLOOD、ICMP_TTL_ZERO_FLOOD、ICMP_TTL_ONE_FLOOD、ICMP_REPLY_FLOOD、ICMP_DESTI_UNREACH_FLOOD、ICMP_REDIRECT_FLOOD、ICMP_ADDR_MASK_REQUEST_FLOOD、ICMP_RECORD_ROUTE_OPTION_FLOOD、ICMP_SECURITY_OPTION_FLOOD、ICMP_STREAM_OPTION_FLOOD、ICMP_TIME_STAMP_OPTION_FLOOD、ICMP_LOOSE_SOURCE_ROUTE_OPTION_FLOOD、ICMP_STRICT_SOURCE_ROUTE_OPTION_FLOOD
	ICMPv6单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送ICMPv6单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 2 种ICMPv6单包攻击：ICMP_FLOOD、ICMP_IP_FRAG_FLOOD
	IGMPv4单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送IGMPv4单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 10 种IGMPv4单包攻击：IP_MULTICAST_FLOOD、IGMPV3_GRAMMAR_FLOOD、IGMPV3_QUERY_FLOOD、IGMPV1_GRAMMAR_FLOOD、IGMPV2_REQUEST_FLOOD、IGMPV2_RESPONSE_FLOOD、IGMPV2_GRAMMAR_FLOOD、IGMPV1_TTL_ZERO_FLOOD、IGMPV2_TTL_ZERO_FLOOD、IGMPV3_TTL_ZERO_FLOOD

DDoS攻击	**ARPv4单包攻击**	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送ARPv4单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 3 种ARPv4单包攻击：ARP_REQUEST_FLOOD、ARP_RESPONSE_FLOOD、ARP_GRAMMAR_FLOOD
	TCPv4单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送TCPv4单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 15 种TCPv4单包攻击：SYN_FLOOD、SYN_ACK_FLOOD、ACK_FLOOD、PUSH_ACK_FLOOD、RESET_FLOOD、FIN_FLOOD、TCP_FRAG_ACK_FLOOD、TCP_IP_FRAG_FLOOD、LAND_ATTACK、TCP_TTL_ZERO_FLOOD、TCP_ERROR_OPTION_FLOOD、TCP_SYN_FIN_FLAG_FLOOD、TCP_NO_FLAG_FLOOD、TCP_FIN_FLAG_FLOOD、TCP_WINNUKE
	TCPv6单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送TCPv6单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 10 种TCPv6单包攻击：SYN_FLOOD、SYN_ACK_FLOOD、ACK_FLOOD、PUSH_ACK_FLOOD、RESET_FLOOD、FIN_FLOOD、TCP_FRAG_ACK_FLOOD、TCP_IP_FRAG_FLOOD、LAND_ATTACK、TCP_WINNUKE
	UDPv4单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送UDPv4单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 9 种UDPv4单包攻击：UDP_MULTICAST_FLOOD、UDP_BROADCAST_FLOOD、UDP_FLOOD、UDP_IP_FRAG_FLOOD、UDP_TTL_ZERO_FLOOD、UDP_ERROR_OPTION_FLOOD、FRAGGLE_ECHO_ATTACK、FRAGGLE_CHARGEN_ATTACK、DHCP_FLOOD
	UDPv6单包攻击	检测受测设备抵御单包攻击的能力，每个虚拟用户以最快速度发送UDPv6单包攻击，尝试耗尽受测设备资源，以致其瘫痪。 当前共包含 3 种UDPv6单包攻击：UDP_FLOOD、UDP_IP_FRAG_FLOOD、DHCP_FLOOD
	未知IP协议报文攻击	检测受测设备抵御未知IP协议报文攻击的能力，每个虚拟用户以最快速度发送未知IP协议报文攻击，尝试耗尽受测设备资源，以致其瘫痪。
	TCP伪装会话攻击	攻击者发送伪造的SYN数据包，ACK数据包，最后是FIN/RST数据包。所有这些数据包类似于从一个主机发送到另一个主机的真实TCP会话流量。
	TCP新建会话攻击	攻击者首先建立大量的有效会话，然后缓慢地响应一个ACK包和不完整的请求，使会话长时间保持打开状态。
	HTTP快速请求攻击	在GET Flood中，攻击者会向目标服务器发送大量有效的GET请求。此类攻击是非欺骗性的，源IP地址是攻击者计算机（或NAT防火墙）的实际IP。此攻击最终将导致被攻击的服务器无响应。
	HTTP变体请求攻击	攻击机器创建多个HTTP请求，不是在一个HTTP会话攻击期间一个接一个地创建请求，而是创建一个包含多个请求的数据包。它是Excessive Verb攻击的一种变体，攻击者可以用低速率的攻击使被攻击服务器CPU负载过高。
	HTTP递归请求攻击	攻击者会识别多个页面或图像生成HTTP GET请求，试图通过递归这些页面或图像模拟正常用户。
	HTTP并发慢确认攻击	检测受测设备抵御长HTTP会话攻击的能力，每个虚拟用户会创建大量有效会话，在开始下载大型文档、对象后，减慢确认速度，从而过度消耗服务器资源。
	HTTP并发慢请求攻击	检测受测设备抵御长HTTP会话攻击的能力，每个虚拟用户在一个HTTP会话中多次请求并降低请求速率，消耗很少的带宽，致使被攻击的服务器无响应。
攻击流量重放	**攻击流量重放**	感知受测设备的入侵检测和防御能力，该测试重放已知的网络攻击数据流，通过检查重放报文的完整性，确定受测设备的入侵检测和防御能力。
防火墙策略检测	**转发策略检测**	尝试与服务器打开指定的端口建立连接，客户端发送syn报文，通过接收服务器的reset或者syn+ack的回应报文，来判断防火墙的策略是阻断还是通过。
	恶意代码检测	通过HTTP协议，Get一个病毒文件或者恶意程序，通过响应的成功与否，判断防火墙对恶意代码的检查结果。
高级模糊检测	**高级模糊测试**	使用先进的模糊技术验证应用程序、主机或网络设备的稳定性。
攻击场景检测	**攻击场景描述语言**	每个虚拟用户，根据特定的场景流量，例如攻击或应用程序交互流量，进行场景模拟，或做为背景流使用。
WiFi无线测试	**IPerf吞吐**	网卡绑定Linux内核驱动，使用开源工具iperf，进行TCP/UDP吞吐测试。
	AB/NGINX新建	网卡绑定Linux内核驱动，使用开源工具ab对nginx服务器，进行HTTP新建测试。

	AB/NGINX并发	网卡绑定Linux内核驱动，使用开源工具ab对nginx服务器，进行HTTP并发测试。
5G核心网测试	**5G核心网测试**	模拟5G核心网信令面业务开始、暂停、恢复、停止等命令，并进行媒体面流量仿真，模拟各种业务类型的数据包，对5G核心网从核心到边缘所有的设备和网络进行测试，获取丢包率、时延等衡量5G核心网数据转发质量的关键参数。
网络流量分析	**报文捕获转发**	从指定网卡上过滤和捕获数据报文，把指定网口设置为混杂模式，过滤和捕获到达此端口的报文，并可快速转发到另外一个端口。
	报文深度解析	用于上传解析捕获的HTTPS报文，识别使用的SSL加密套件。
	并发扫描检测	根据国家发布的网络关键设备和网络安全专用产品的检测要求，对网络脆弱性扫描产品，要求最大并行扫描IP数量大于等于60个，进行检测认证。