Supernova 测试仪功能列表				
分类			用例	功能介绍
L4-7协议测试	Web协议测试	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。 用户模式：对于延迟低、转包快的受测设备，可以获得更好的测试结果，因为每个虚拟用户对应合适的收发队列，其执行流程能快速完成，所以获得最佳性能要调整虚拟用户数量，此模式在最佳用户时会获得更好的性能。 强打模式：使用高精度定时器，按固定速率执行新建流程，即TCP三路握手->HTTP请求响应->关闭TCP连接，如果受测设备不能完成指定的新建速率，将会有新建失败的统计。 对于队列优化，能同时承受快速新建、大量并发、高吞吐率的受测设备，可以获得更好的测试结果，因为测试仪均衡输出了新建、并发、吞吐的压力，只要受测设备能快速处理报文和请求，不触发测试仪超时重传等出错机制，就能同时获得良好的新建、并发、吞吐性能。
			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。
		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每秒握手速率	每个虚拟用户新建一条 TCP连接，然后进行SSL握手，SSL握手完成后，直接关闭SSL和TCP连接，不发送HTTP请求和接收响应。
		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。
		HTTP3	HTTP3每秒新建会话	客户端基于开源 QUIC协议库lsquic 创建HTTP3会话请求，获取受测设备新建会话的最快速率，每个虚拟用户建立一条 connection连接，完成一次完整的 HTTP3事务(发送请求和接收回应)，最后关闭连接，再新建connection 并包含一次完整的 HTTP3会话。
			HTTP3最大吞吐速率	客户端基于开源 QUIC协议库lsquic 创建HTTP3会话请求，获取受测设备HTTP3的最大吞吐量，每个虚拟用户建立一条 connection连接，循环完成HTTP2事务(发送请求和接收回应)，最后关闭连接。
		WebSocket	WebSocket请求处理	获取受测设备处理 WebSocket消息的能力。客户端模拟大量虚拟用户，发送HTTP请求与WebSocket服务器建立长连接，在保持长连接条件下不断发送 WebSocket消息帧。
		浏览器	浏览器流量测试	模拟真实浏览器访问页面的行为，通过模拟大量同时并发的浏览器请求，测试Web隔离等防护产品的相关性能指标
	视频协议测试	RTSP/RTP/RTCP	视频点播速率	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。流量如：优酷、爱奇艺的视频点播。
			视频传输质量	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。流量如：优酷、爱奇艺的视频点播。
			视频并发数量	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。流量如：优酷、爱奇艺的视频点播。
			视频流量传输	获取受测设备处理视频流媒体的并发量和吞吐量。每个虚拟用户循环播放视频流媒体，虚拟用户数量就是视频播放的并发量。支持的视频编码格式有 :H264 和H265。
			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ITU-T P.862建议书提供的 PESQ(Perceptual Evaluation of Speech Quality)方法，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。
		HLS	HLS流媒体播放	HTTP Live Streaming (缩写是HLS)是基于HTTP的流媒体网络传输协议，它的工作原理是把整个流分成一个个小的基于 HTTP的文件来下载，每次只下载一些。当媒体流正在播放时，客户端可以选择从许多不同的备用源中以不同的速率下载同样的资源，允许流媒体会话适应不同的数据速率。
		RTMP	RTMP流媒体播放	RTMP是一种设计用来进行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。
		GB28181	GB28181监控视频流量传输	GB/T28181《安全防范视频监控联网系统信息传输、交换、控制技术要求》，是由公安部科技信息化局提出，由全国安全防范报警系统标准化技术委员会 (SAC/TC100)归口，公安部一所等多家单位共同起草的一部国家标准。分为客户端和服务端，客户端模拟多路摄像头，服务端模拟上级管理平台，支持模拟GB28181 协议（注册、心跳、点播、推流等信令），支持模拟指定数量摄像头和设置码流 （标清2M、高清4M、超高清8M等），视频编码h264、h265
	邮件协议	SMTP	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。
		SMTPS	SMTPS邮件发送速率	获取受测设备处理邮件发送的最快速率，通过模拟大量虚拟用户，循环建立TCP连接并进行 SSL握手，使用SMTP完成电子邮件的发送，最后关闭TCP连接。
		POP3	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	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。
	工控协议	MODBUS	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	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。
		S7COMM	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。
		IEC61850_MMS	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。
		S7	S7	建立S7COMM连接，进行报文的发送和接收，模拟S7COMM协议仿真测试。
		DNP3	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。
		IEC61850	IEC61850	实现在向网络或 IED设备施加压力流量的同时，输出SV、GOOSE报文，进行短路及故障模拟，测试保护动作性能及智能终端传输延时。
	UDP/TCP 测试	UDP	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。
		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。
	4-7层协议仿真	数据库协议	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。
		基于TCP的协议	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。
			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	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	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。
		基于UDP的协议	Syslog	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。
			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。
		DHCP协议	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协议	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_TCP	通过TCP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 TCP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_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 。	
			DNS_over_TLS	通过TLS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 TLS发送DNS请求并接收回应，计算请求的成功率和时延 。	
		SIP协议	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 。	
	通用协议承载	新建	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。	
		吞吐	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。	
		并发	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。	
	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。	
L2-3协议测试	动态路由协议	RIPv1v2	RIP路由建成数量	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	RIP路由建成数量	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	OSPFv2路由建成数量	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	OSPFv3路由建成数量	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	BGPv4路由建成数量	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+	BGP4+路由建成数量	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	ISISv4路由建成数量	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 。	
		ISISv6	ISISv6路由建成数量	在测试仪端口上模拟支持 ISISv6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 。	*客户使用时支持
	组播协议	IGMP	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	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。	
		PIM	PIM-DM组播处理	PIM(Protocol Independent Multicast)是一种独立的组播协议，旨在解决IP组播路由问题。它允许网络设备在不维护特定单播路由信息的情况下 ，利用现有的单播路由表来构建和维护组播树。PIM协议的主要特点是其独立于特定的单播路由协议 ，如OSPF,IS-IS或BGP,这使得它能够更灵活地适应不同的网络环境 。 PIM-DM通过周期性"扩散-剪枝"维护一棵连接组播源和组成员的单向无环 SPT。适合规模较小、组播组成员相对比较密集的局域网 。	
		PIMSm	PIM-SM组播处理	PIM(Protocol Independent Multicast)是一种独立的组播协议，旨在解决IP组播路由问题。它允许网络设备在不维护特定单播路由信息的情况下 ，利用现有的单播路由表来构建和维护组播树。PIM协议的主要特点是其独立于特定的单播路由协议 ，如OSPF,IS-IS或BGP,这使得它能够更灵活地适应不同的网络环境 。 PIM-SM采用接收者主动加入的方式建立组播分发树 ，需要维护RP、构建RPT，注册组播源。适合网络中的组成员相对比较稀疏 、分布广泛的大型网络 。	
		PIMSsm	PIM-SSM组播处理	PIM(Protocol Independent Multicast)是一种独立的组播协议，旨在解决IP组播路由问题。它允许网络设备在不维护特定单播路由信息的情况下 ，利用现有的单播路由表来构建和维护组播树。PIM协议的主要特点是其独立于特定的单播路由协议 ，如OSPF,IS-IS或BGP,这使得它能够更灵活地适应不同的网络环境 。 PIM-SSM是对传统PIM协议的扩展，直接在组播源与组成员之间建立 SPT，无需维护RP、构建RPT。注册组播源。适合网络中的用户预先知道组播源的位置 ，直接向指定的组播源请求组播数据的场景 。	
	2-3层协议仿真	PCAP发送	PCAP发送	遍历所有pcap文件，读取所有的报文信息，在一个端口上发出 。注意此发送为有序无状态重放 ，不会按TCP/UDP流区分客户端和服务端网口 ，只是将报文在端口上发送 。	
		PPPoE协议	PPPoE	PPPoE（点对点协议 over Ethernet）是在以太网上建立点对点连接的一种通信协议 ，其过程包括建立并认证会话 、分配IP地址、生成路由并进行数据传输 。	
		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。	
		SRv6协议	L3 EVPN Over SRv6	通过IPv6网络透明传输用户三层数据 ，实现属于同一个 VPN、位于不同地理位置的用户互通 。	
			VPWS Over SRv6	在基于SRv6协议的公网上建立点到点的虚拟专线技术	
			VPLS Over SRv6	在基于SRv6协议的公网上为不同地域的各分支机构提供 L2VPN业务	
		VXLAN协议	BGP_EVPN	通过扩展BGP协议，使用扩展后的Type5路由可达性信息，把Vxlan隧道信息同步给受测设备 。支持16M的虚拟隧道数，采用MAC in UDP的报文封装技术，实现大二层的虚拟局域网。	
		NETCONF	NETCONF	基于开源软件库 libnetconf2，及其扩展工具集 Netopeer2，通过NETCONF 协议对网络设备进行测试 。	*当前版本开发在调试
	RFC基准测试	RFC2544	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	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，监听端口监听迂洪帧或者转发错误帧，通过二分法的应用可确定 DUT在无迂洪和无错误转发情况下 ，正确学习并转发的最大地址数 。	
			RFC2889 MAC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 。监听端口监听迂洪帧或者转发错误帧 。通过二分法的应用可确定 DUT在无迂洪和无错误转发情况下的最大学习速率 （单位为帧每秒 ）。	
			RFC2889转发测试	在可以丢包的情况下 ，设备能够接收并转发的最大数据速率 。	*客户使用时支持
		RFC3918	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 。	
			v4组转发矩阵测试	确定DUT/SUT 在一定数量端口加入不同数量的组播组时的转发率 。	
	VPN隧道测试	IPSec VPN	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。	
	网络流量重放	流模板	流模板	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。	
		流量重放	PCAP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 。	
专用网络测试	智算网络测试	RoCEv2 协议测试	RoCEv2_Perftest	RoCE(RDMA over Converged Ethernet)，即基于以太网的 RDMA技术，允许在不依赖 InfiniBand专用硬件的情况下使用 RDMA，RoCE v2版本基于以太网的 UDP协议，UDP目标端口4791保留给RoCE v2流量，将IB的传输层作为UDP的payload（即TCP/IP协议栈的应用层）数据。物理测试仪配套 NVIDIA的Connect-X系列的高性能网卡 ，可以支持rdma-core库使用测试仪集成的 perftest开源工具，发送和接收RoCEv2的流量，对支持RoCEv2的网络设备进行测试 。物理测试仪搭配 FPGA系列网卡，使用硬件时间戳控制时延，精度可以达到10纳秒级别，可以对支持RoCEv2的高性能交换机进行测试 。	
			RoCEv2_QP_新建	RoCE(RDMA over Converged Ethernet)，即基于以太网的 RDMA技术，允许在不依赖 InfiniBand专用硬件的情况下使用 RDMA，RoCE v2版本基于以太网的 UDP协议，UDP目标端口4791保留给RoCE v2流量，将IB的传输层作为UDP的payload(即TCP/IP协议栈的应用层）数据。 每个虚拟用户依据 CM管理协议创建一个 ROCE连接，发送和接收指定长度的数据，然后关闭CM连接，不断地重复这个过程，物理测试仪搭配FPGA系列网卡，使用硬件时间戳控制时延，精度可以达到 10纳秒级别，可以对支持RoCEv2的高性能交换机进行测试。单臂模式可以与 rdma_client或rdma_server 工具互通 。	
			RoCEv2_吞吐时延	RoCE(RDMA overConverged Ethernet)，即基于以太网的 RDMA技术，允许在不依赖infiniBand 专用硬件的情况下使用 RDMA，RoCE v2版本基于以太网的 UDP协议，UDP目标端口4791保留给 RoCE v2流量，将IB的传输层作为 UDP的pavoad(即TCP/IP协议栈的应用层）数据。 此用例(使用DPDK用户态收发报文模式，封装RoCEv2报文和实现RDMA握落流控，重传确认，稳定传输，测试网络设备或者 RDMA网卡，物理测试仪搭配FPGA系列网卡，使用硬件时间戳控制时延，精度可以达到 10纳秒级别，可以对支持RoCEv2的高性能交换机进行测试 。在单臂测试时，可以与perftest工具进行对接测试 。	
			RoCEv2_集群组合	模拟NCCL库（NVIDIA Collective Communications Library），优化在多GPU和多计算节点环境中进行并行计算的网络通信 。用例提供了一组基本的集合通信操作 （Collective Communication Primitives），如广播（Broadcast）、全收集（All-gather）、全归约（All-reduce）、规约散播（Reduce-scatter）等，这些操作对于进行大规模并行处理和深度学习训练非常关键 。	
			RoCEv2_异常测试	RoCE(RDMA over Converged Ethernet)，即基于以太网的 RDMA技术，允许在不依赖 infiniBand专用硬件的情况下使用 RDMA，RoCE v2版本基于以太网的UDP协议，UDP目标端口4791保留给 RoCE v2流量，将IB的传输层作为 UDP的pavoad(即TCP/IP协议栈的应用层）数据。此用例可以模拟一些异常测试 ，模拟不同的异常测试时 ，发送对应的异常报文 。	
			RoCEv2_Nak 攻击测试	测试仪能够模拟发送 ROCE_NAK攻击报文，旨在对被测设备进行 NAK泛洪攻击测试 。通过发送大量的ROCE NAK（Negative Acknowledgment ）消息，测试仪可以干扰或中断被测设备的正常通信，导致设备出现性能问题或通信故障 。	

	5G核心网测试		5G信令面仿真测试	5G信令仿真测试组件基于自主研发的协议栈仿真平台 ， 采用微服务架构，根据3GPP R15/R16/R17/R18 相关协议技术标准规范 ，支持仿真gNB+UE的N1/N2接口，可灵活的编辑协议栈消息，灵活的选择消息所携带的信元 ，灵活的构造业务流程 ，通过编写大量测试脚本 ，实现仿真UE、gNB与5G核心网进行注册 ，会话建立 ，切换 ，服务请求等信令业务流程，并在信令交互过程中 ，分析核心网响应的信令消息 ，判断信令流程是否符合协议规范 。
			5G性能测试	5G核心网测试组件基于自主研发的协议栈仿真平台 ，采用微服务架构，配合业务面流量仿真 ，通过模拟各种业务类型的数据流量包 ，根据3GPP R15/R16/R17/R18 相关协议技术标准规范，快速堆叠5G业务仿真线程，通过增加5G用户规模 ，构造5G用户面媒体流量数据内容 ，实现针对5G系统高性能的压力测试 。
			5G功能测试	5G核心网测试组件基于自主研发的协议栈仿真平台 ，采用微服务架构，根据3GPP R15/R16/R17/R18 相关协议技术标准规范 ，通过5G协议栈消息编辑器 ，可灵活选择消息所携带的信元 ，配置信元参数值和输入来源 ，使用定制化流程编辑工具 ，快速构造5G标准和异常业务流程 ，实现仿真UE、gNB与5G核心网进行注册 ，会话建立 ，切换，服务请求等信令业务流程，并在信令交互过程中 ，分析核心网响应的信令消息 ，判断信令流程是否符合协议规范 。
			5G信令风暴	信令风暴主要是由于设计不当或行为不当的 5G设备/终端/应用，频繁申请业务 、建立和断开数据连接以及非正常的消息和流程所致 。 信令风暴测试基于5G标准业务，模拟极端场景的特征和规模 ，通过海量信令请求来验证被测 5G 系统的健壮性和鲁棒性 。 为了准确地实现信令风暴的测试要求 ，5G核心网测试组件基于自主研发的协议栈仿真平台 ，采用微服务架构可以实现完整的 5G标准信令过程，可灵活构造信令风暴模型 ，根据不同的测试场景，选择不同的业务流程组合 ，针对性地对5G被测系统发起信令风暴 ，通过统计结果反馈出各项指标从而评估被测设备抗信令风暴能力 。
			5G网元仿真测试	5G网元仿真测试组件基于自主研发的协议栈仿真平台 ，采用微服务架构，根据3GPP的相关协议规范 ，模拟5G无线通信网络相关网元 ，对真实的被测网元或设备进行功能和性能测试 。基于Web友好参数配置操作界面 ，可以灵活配置各基础网元参数信息 ，通过脚本定义模拟 5G核心网系统中各网元之间的协议栈信息和消息交互 ，仿真模拟网元间业务流程，按照设定的话务模型或测试用例触发其业务流程 。
	卫星通信测试	NTN 网络测试	基站连接业务测试	测试仪表依据3GPP协议标准，基于3GPP用户面GTP-U协议封装，提供VLAN、VXLAN和DSCP隧道封装方式模拟正常场景和拥塞场景 ，仿真终端、基站和核心网，基于卫星通信网络拓扑模板定义整个网络 ，灵活配置终端数量 、模拟终端网络 IP地址，构造星状网业务负载内容 ，建立卫星链路上下行业务流量 ，对单独终端业务数据情况及全部终端总业务数据情况进行统计，从而验证NTN网络基站业务质量 。
网络安全测试	系统安全测试	系统漏洞扫描	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 。
		Web攻击靶场	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	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 。
		DDoS单包攻击	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
			ICMP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 ICMP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ICMP单包攻击：ICMP_FLOOD （支持双栈测试 ）、ICMP_IP_FRAG_FLOOD （支持双栈测试 ）、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
			IGMP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
			ARP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
			TCP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 14 种TCP单包攻击：SYN_FLOOD （支持双栈测试，ipv6协议帧长范围为 78-9018 ）、SYN_ACK_FLOOD （支持双栈测试，ipv6协议帧长范围为 78-9018 ）、ACK_FLOOD（支持双栈测试，ipv6协议帧长范围为 78-9018 ）、PUSH_ACK_FLOOD （支持双栈测试，ipv6协议帧长范围为 78-9018 ）、RESET_FLOOD（支持双栈测试，ipv6协议帧长范围为 78-9018 ）、FIN_FLOOD（支持双栈测试，ipv6协议帧长范围为 78-9018 ）、TCP_FRAG_ACK_FLOOD （支持双栈测试，ipv6协议帧长范围为 78-9018 ）、TCP_IP_FRAG_FLOOD （支持双栈测试，ipv6协议帧长范围为 82-9018 ）、LAND_ATTACK （支持双栈测试，ipv6协议帧长范围为 82-9018 ）、TCP_TTL_ZERO_FLOOD 、TCP_ERROR_OPTION_FLOOD 、TCP_SYN_FIN_FLAG_FLOOD 、TCP_NO_FLAG_FLOOD 、TCP_FIN_FLAG_FLOOD
			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 UDP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UDP单包攻击：UDP_MULTICAST_FLOOD （仅支持ipv4）、UDP_BROADCAST_FLOOD （仅支持ipv4）、UDP_FLOOD （支持双栈测试，ipv6协议帧长范围为64-9018 ）、UDP_IP_FRAG_FLOOD （支持双栈测试，ipv6协议帧长范围为 64-9018 ）、UDP_TTL_ZERO_FLOOD （仅支持ipv4）、UDP_ERROR_OPTION_FLOOD （仅支持ipv4）、FRAGGLE_ECHO_ATTACK （仅支持ipv4）、FRAGGLE_CHARGEN_ATTACK （仅支持ipv4）、DHCP_FLOOD（支持双栈测试，ipv6协议帧长范围为 64-9018 ）、UDP_EXCEPTION_EXTENSION_HEADER_FLOOD （仅支持ipv4）
			UDP载荷攻击	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 UDP载荷攻击，尝试耗尽受测设备资源 ，以致其瘫痪 。可以自定义载荷内容 。
			SIP单包攻击	攻击者通过发送大量的 register消息到SIP服务器，导致被攻击SIP服务器分配大量的资源用以记录和跟踪会话 ，直到资源耗尽而无法响应合法用户的注册请求 。SIP服务器可开启学习模式进行防护 。 当前共包含2种SIP单包攻击：SIP_REGISTER_FLOOD 、SIP_INVITE_FLOOD
			DNS请求攻击	每个虚拟用户向DNS服务器发送一个请求 ，对一个随机URL进行ANY类型查询，并等待DNS服务器的响应 ，循环往复，对DNS服务器进行攻击 。
			DNS放大攻击	客户端模仿DNS服务器，向被攻击对象（服务端）发送大量DNS响应，使受攻击对象网络严重阻塞 ，导致网络崩溃或者服务中断 。
			SSDP放大攻击	SSDP放大攻击是一种利用 SSDP协议弱点的网络攻击方法 。攻击者通过伪造 IP地址，向网络上的SSDP设备发送大量查询请求 ，并将响应数据包放大 ，从而将流量放大多倍 ，最终使目标主机网络不可用 。SSDP放大攻击属于 DDoS攻击的一种，因为攻击者会通过各种手段让多个设备同时发送请求 ，从而造成网络瘫痪 。
			NTP放大攻击	NTP放大攻击 (NTP Amplification Attack), 是一种利用NTP(网络时间协议) MON_GETLIST 查询功能的漏洞，对目标计算机进行 DDoS(分布式拒绝服务)攻击的方式。测试仪通过伪造大量的IP地址和用户, 发送Monlist查询请求到目标服务器，该请求会让NTP服务器不断地向指定目标 IP地址发送巨大的响应包，占用大量带宽，影响正常业务，最终导致网络瘫痪 。
			MEMCACHED 放大攻击	客户端向 memcached 服务器发送 get请求，并伪造源ip地址，来使得memcached 服务器对伪造的 ip地址发送大量的响应报文 ，导致被攻击的设备网络崩溃或服务中断
			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 。
		DDoS会话攻击	HTTP FlOOD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 。
			HTTPS FLOOD攻击	在进行SSL连接并握手之后 ，反复不断的进行密钥重新协商过程 ，造成被攻击目标资源耗尽
			HTTP慢速攻击	攻击者建立TCP连接后，缓慢发送HTTP请求，占用并耗尽服务器的资源 。
			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 。
			TCPWinnuke 攻击	WinNuke攻击是一种拒绝服务攻击 。向端口发送一些携带 TCP带外数据(out of band, OOB)报文，使Windows95瞬间蓝屏，并且网络功能完全瘫痪 。
			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 。
		网络风暴测试	单播风暴攻击	当网络中存在不对称路由 （Asymmetric Routing），或交换机生成树拓扑改变 （Spanning-Tree Protocol Topology Changes），或交换机转发表溢出 （Forwarding Table Overflow）时，网络中会出现大量的单播报文 ，这些单播报文 ，也会造成交换机发送大量泛洪 ，使网络处理能力受到严重影响 。测试仪模拟这样的场景 ，发送大量的单播报文 ，造成交换机泛洪，严重影响网络性能 ，或者导致网络瘫痪 。
			广播风暴攻击	当网络受到如蠕虫病毒攻击时 或者存在交换机端口故障 、网卡故障、链路冗余没有启用生成树协议 、网线线序错误或受到干扰等问题时 ，一个数据包或帧被传送到本地网段 (由广播域定义)上的每个节点就是广播，广播风暴就是网络上的存在的大量被转发的广播帧 ，数量急剧增加而出现无法正常网络通信的反常现象 。测试仪模拟发送大量的 ARP广播报文，导致广播报文泛洪 ，会占用相当可观的网络带宽 ，严重影响网络性能 ，或者导致网络瘫痪 。
			组播风暴攻击	组播是把从一个由源产生的报文发送给一组目的 IP(224.0.0.0-239.255.255.255 这样的D类地址)。在一个特定的路由器上 ，一个包要多个备份可能从多个接口上发出 。如果有环路存在，那么一个或多个包会返回到其输入的接口 ，而且这个包也会经复制发到其他的端口上 。这一结果可能导致多播风暴 。测试仪模拟发送能造成环路的多播报文 ，如果存在环路包就会不断在路由器与交换机间复制 ，严重影响网络性能 ，或者导致网络瘫痪 。
			SV风暴测试	SV风暴测试用例，高速发送重复的sv报文，或者发送变化字节的 sv报文，如mac地址的改变
			GOOSE风暴测试	GOOSE风暴测试用例，高速发送重复的GOOSE报文，或者发送变化字节的 GOOSE报文，如mac地址、sq、st
			MMS风暴测试	MMS风暴测试（模拟同时使用不同 IP地址的MMS客户端同时连接装置并发送 connectrequest），MMS召唤风暴（模拟最大32个客户端连接被测装置，所有客户端以最小间隔重复读取定值信息），MMS报告风暴（模拟最大32个客户端连接被测装置，所有客户端以最小间隔循环召唤报告 ）
			LLDP风暴测试	LLDP风暴测试用例，高速发送重复的报文 。
		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 。系统预置攻击报文数量 10916个，涉及HTTP、HTTPS、UDP、SMTP、Microsoft、MySQL、Oracle、DNS等攻击类型。
		加密解密验证	加密解密验证	使用指定的对称/非对称加密算法，对原始数据进行加密或解密运算 。使用指定的hash算法，对原始文本进行摘要计算 。使用此功能可以进行加密解密或摘要验证 。
		国密接口测试	国密接口测试	对符合GMT0018 规范的密码设备进行性能测试 。包括密码存储容量和对称 、非对称、杂凑等国密算法的性能测试 。
		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 。
		Web站点扫描	web站点扫描	对目标服务器进行目录扫描 ，查找隐藏在目标服务器里的目录和文件
		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 。
		动态防护测试	动态防护测试	使用动态防护检测组件和靶场软件 ，模拟真实的浏览器 ，检测Web动态防护产品的功能和性能 。
			密钥计算能力	使用sysbench 1.0.20测试主机性能，包括CPU处理能力、内存和硬盘访问速度 、MySQL 数据库处理能力 。

测试分析工具	**CPU算力测试**	**浮点数计算能力**	mt-dgemm用来获取计算机系统或特定运算的计算性能的指标 。测试原理为两个N*N的矩阵相乘， 矩阵乘积的第m行第n列的元素等于矩阵1的第m行的元素与矩阵2的第n列对应元素乘积之和。矩阵乘法时间复杂度为 O(N×N×N)。重复测试次数是重复执行基准测试 ， 确保处理器性能一致， 不受热节流的影响 。mt-dgemm通过执行重复测试次数 ×N×N×N次浮点乘法和加法计算来获取 GFLOPS值。
	内存访问测试	**内存访问速度**	使用Stream5.10测试主机内存带宽性能
	硬盘访问测试	**fio**	使用fio 3.35，测试测试仪主机文件系统或块设备基准性能
		vdbench	使用Vdbench 5.04.07，测试测试仪主机文件系统或块设备基准性能
	常用工具测试	**JMeter**	基于Supernova的Jmeter组件使用JDK 1.8.0和Jmeter 5.5.0，可以在测试仪Linux环境中直接运行 Jmeter进行测试。
		IPerf	网卡绑定Linux内核驱动，使用开源工具iperf 2.1.8，进行TCP/UDP吞吐测试。
		ab/nginx	网卡绑定Linux内核驱动，使用开源工具ab对nginx服务器，进行HTTP测试。
		UPerf	使用开源工具uperf 1.0.7，来模拟多个TCP连接并测量其性能。
	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 。
		业务系统拨测	将测试仪当作探针， 通过模拟不同协议的客户端向服务端发送请求 ， 来实现监控服务端状态的功能 。可以满足对客户端请求的内容进行配置 ， 以及对服务端响应内容中关键信息的解析。