

DarPeng2000E Application and Security Tester



DarPeng2000E is high-performance application and security tester launched by Xinertel for voice, video, data applications, and network security test. It accurately simulates the network access behavior of millions of real end users, and performs pressure and performance tests on application and security devices(such as Firewall/IPS/IDS/WAF/DPI, etc.) or the entire system;By simulating a large amount of real attack traffic and malicious software and virus traffic, the detection and defense capabilities of network security devices and systems against attacks and viruses can be verified and tested. At the same time, the control and recognition capabilities of the tested device over traffic can be confirmed by replaying real environment traffic.

Collaborating with B/S architecture testing software ALPS(Application Layer Protocol Simulator), which supports real application layer traffic simulation(such as application layer protocol HTTP/FTP/TCP/DNS, voice: VoIP SIP&RTP, video: RSTP/RTP/IPTV, etc.), its HTTP/TCP can create millions of new connections and billions of concurrent connections; ALPS can simulate real attack traffic(DDoS attacks/botnets/custom attacks, etc.), malicious traffic, virus traffic. And ALPS supports audio and video quality testing.

Key Features

• Comprehensive interfaces

Supports up to 4 100GE QSFP28 ports(compatible with 50G, 40G, 25G, 10G), 16 SFP+10GE ports, or 32 SFP 1GE ports, allows mixed installation of test modules with varying data rates

• Ultra high application protocol simulation capability

TCP Performance:

8 million TCP CPS, 300 million TCP CC;

HTTP Performance:

6.4 million HTTP CPS, 200 million HTTP CC, and 194G HTTP throughput.

HTTPS Performance:

270000 HTTPS CPS, 7 million HTTPS CC, and 100G HTTPS throughput;

• Support network security device performance and capacity testing

Including firewalls, load balancers, WAFs, URL filters, antivirus, anti spyware, HTTP/HTTPS accelerators, WAN accelerators, IDS/IPS, and IPsec VPN gateways, etc

• Support application server performance testing

Including web servers, mail servers, DHCP services, FTP servers, DNS servers, RTSP/RTP QuickTime streaming servers, multicast servers, etc

• Support network security testing

Support simulation of attack traffic, virus traffic, and Cyber Range.

• Support offline testing

Enables offline testing, ensuring that test results are not lost in the event of management network disconnections.

Specifications

Port and Speed	<ul style="list-style-type: none"> Up to 4 QSFP28 100G(compatible with 50G, 40G, 25G, 10G) Up to 16 SFP+ 10G/1G Up to 32 SFP/RJ45 1G
Dimensions (W×H×D)	3U: 438mm x 132mm x 500mm
Rack Mount	Mounted in rack that meets the IEC 297 standard: <ul style="list-style-type: none"> Width: 19 inches Depth: ≥ 800 mm
Weight(kg)	15.5KG
Temperature	0°C ~ 40°C
Power	AC 110~230V; 50Hz; 10A
Max power consumption(W)	1500

Protocols

Application	TCP, UDP, SCTP, WebSocket, DNS, HTTP, HTTPS, HTTP2, FTP, SSH, Telnet TFTP, RTMP, H.225, H.245, SMB, RPC, ONVIF, Chat applications(SKYPE, QQ, WeChat, etc.), E-mail applications(SMTP, POP3, IMAP, etc.), Gaming applications, video applications(HLS, etc.), Download applications(BitTorrent, eDonkey, etc.), Social news applications(Tiktok etc.), Payment applications, Database applications(Oracle, MySQL, MSSQL, etc.)
Industrial control protocol	ECHONET Lite, BACnet, Modbus, OPCUA, MQTT, ProfiNet(PNIO CM), OPC DA, IEC104, EtherNet/IP, ProfiNet(DCP), ENIP, IEEE C37.118 Synchronizer Omron Fins, S7comm, DNP3, Ether-S-I/O, CoAP
Voice	SIP/RTP, Voice Codec (PCMU, PCMA, G.723, G.728, G.729, G.726-32, G.729AB, G.729A, G.723.1), MOS score
Video	RTSP/RTP, Multicast, Video Codec(H.261, H.262/MPEG-2, H.263, H.264, H.265, MPEG-TS, MPEG-1, MPEG-4)
DDoS	Support more than 90 types of DDoS attacks, including L2/L4 DDoS attacks(ARP/ICMP/UDP/TCP/IP/ IGMP, etc.) and L7 Application Attacks(DNS Reflection, Slowloris slow attacks, etc.)
Virus and attack libraries	Covering over 7000 types of vulnerability attacks, over 40000 types of virus, and 73 types of DDoS attacks. The virus and attack library is updated on a monthly basis.
Access Protocol	IPv4, IPv6, 802.1Q(QinQ), DHCPv4/DHCPv6 client, DHCPv4/DHCPv6 server, PPPoEv4/PPPoEv6 client, PPPoEv4/PPPoEv6 server, IPsecv4/IPsecv6, GTP, 802.1x, IP/TCP+UDP/TCP/UDP, custom IPv6 extension headers and stream labels
Routing Protocol	SRv6 BE/SRv6 TE
Data encryption and decryption	SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3

Ordering information

Product Name	Product Description	Product Classification
DarPeng2000E	DarPeng2000E Appliance, support up to 8 slots	Chassis
K2-100G-1QSFP28-HQ	1 port 100G/50G/40G/25G/10G five speed high-performance test module	Test Module
K2-10G-4F-HD	4 ports SFP+ 10G/1G two speed high-performance test module	Test Module
K2-1G-4F-HS	4 ports SFP 1G high-performance test module	Test Module
K2-1G-4C-HT	4 ports RJ45 1G high-performance test module, support 10M/100M/1000M	Test Module
ALPS Security and Protocol Software Package A	Compatible with the DarPeng platform, supporting all components, including virus and attack library updates during the valid maintenance period. Capable of handling all attack and application types, including HTTP, FTP, replay, DDoS, virus, and other attack scenarios.	DarPeng Series License