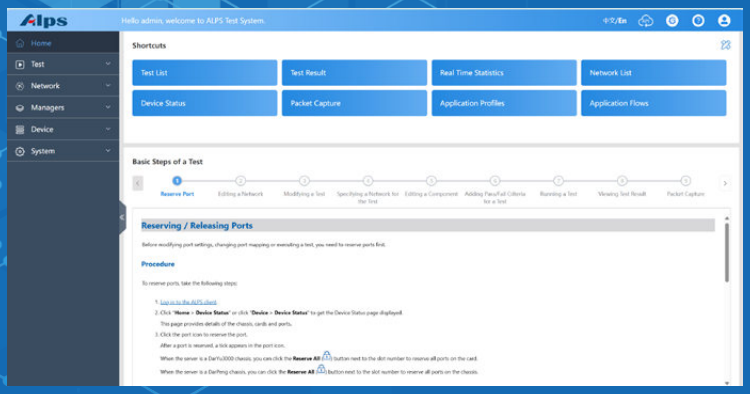


ALPS

L4-7 application and security testing software

As a professional provider of L47 layer testing solutions, Xinretel has launched a new generation of L4 - 7 testing software platform ALPS based on Web- oriented PCT architecture, which can meet the current application and security testing scenarios needs of the majority of network security equipment manufact urers(including firewalls, IPS/ IDS, WAF, SLB, DPI, etc.), telecom operators, and various research institutions. ALPS new platform in The usability, functionality, and scalability have been greatly improved.

ALPS can simulate data, voice, and real users behavior, accurately emulating millions of real end-user and network behaviors. It can conduct stress and performance testing for individual application layer-aware devices(such as Firewall/ IPS/IDS/WAF/DPI, etc.) or entire systems. It can simulate a large amount of real attack traffic and malicious virus traffic, verifying and testing the detection and defense capabilities of network security devices and systems against attacks and viruses, providing important performance and effectiveness evaluations for security testing.

Key Features

- Supports 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
- Supports application server performance testing: web servers, mail servers, DHCP services, FTP servers, DNS servers, RTSP/RTP QuickTime streaming servers, multicast servers, etc
- Supports network security testing: Simulation of thousands of attack traffic types, Fuzzing testing, malware&virus and cyber range

Platform Advantages

◆ **Ease of Use**

ALPS utilizes a unified, streamlined web-based user interface to perform operations such as test configuration, test execution, user management, test case management, device management, and test result presentation and management. In addition, comprehensive help documentation and convenient log query functions make it easier for new users to get started.

◆ **Functionality**

The diversity of application protocols, flexibility in protocol configuration, and customizability of protocol behavior significantly enhance the realism of traffic simulation to meet customer requirements.

During test execution, users can view real-time statistics, define pass/fail criteria, and generate comprehensive test reports upon completion, covering detailed information from the test environment and configurations to statistical data and results.

◆ **Maintainability**

A built-in monitoring system continuously tracks the health status of the simulation platform by collecting, reporting, and storing real-time data on CPU, memory, and disk usage. It also provides early warnings for potential environmental anomalies, helping to prevent test failures caused by system issues, thereby ensuring high maintainability. In addition, detailed platform logs are available to assist with issue diagnosis.

◆ **Scalability**

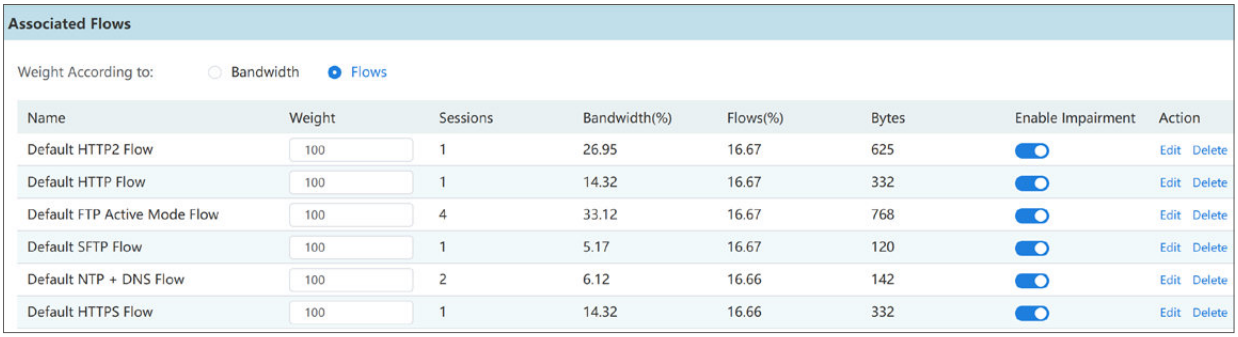
ALPS features a modular software architecture, enabling rapid support for new protocol simulation as well as functional expansion and customization across different protocol layers.

◆ **Customizable Services**

Based on the existing software and hardware platforms, we provide testing services for proprietary technologies and protocols according to customer requirements.

Multiple application protocol emulation

HTTP/HTTPS/DNS/FTP protocols, private, non-standard protocols(capture and playback)



Associated Flows

Weight According to: Bandwidth Flows

Name	Weight	Sessions	Bandwidth(%)	Flows(%)	Bytes	Enable Impairment	Action
Default HTTP2 Flow	100	1	26.95	16.67	625		Edit Delete
Default HTTP Flow	100	1	14.32	16.67	332		Edit Delete
Default FTP Active Mode Flow	100	4	33.12	16.67	768		Edit Delete
Default SFTP Flow	100	1	5.17	16.67	120		Edit Delete
Default NTP + DNS Flow	100	2	6.12	16.66	142		Edit Delete
Default HTTPS Flow	100	1	14.32	16.66	332		Edit Delete

Supports multiple types of DDoS attacks, including TCP, UDP, ARP, ICMP, and IP

Basic Info

* Name: DDoS Attack Description:

Associated DDoS Attack Flows Delete +Add

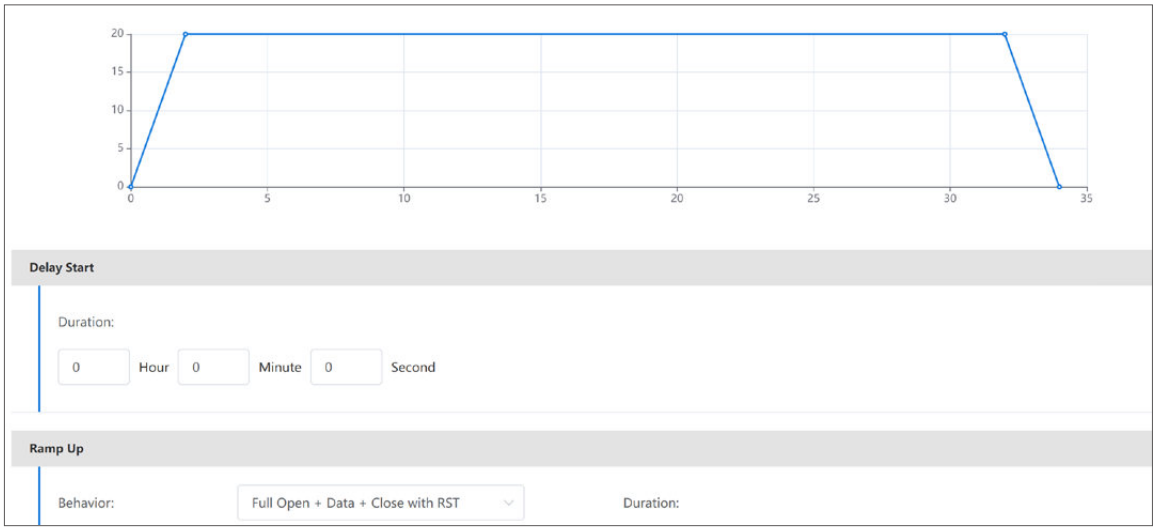
Weight According to: Bandwidth Flows

Name	Weight	Sessions	Bandwidth(%)	Flows(%)	Bytes	Action
Default TCP DDoS Attack Flow	50	13	0.88	20.00	2344	Edit Delete
Default UDP DDoS Attack Flow	50	5	0.68	20.00	1812	Edit Delete
Default ARP DDoS Attack Flow	50	1	0.02	20.00	46	Edit Delete
Default ICMP Flood DDoS Attack Flow	50	1	0.06	20.00	160	Edit Delete
Default IP DDoS Attack Flow	50	5	98.37	20.00	262570	Edit Delete

Total 5 1

Real User simulation

- Real, multi-protocol traffic models
- application mix and bandwidth control
- L4-7 stateful application traffic emulation



Real-time statistics and packet capture