Datasheet

Dotouch 触点互动

XproNetworkSimulator (XproNS)

All-in-one applications and network security testing solution

Dotouch XproNetworkSimulator (XproNS) application and security testing solution delivers the industry's most comprehensive and trusted L4-7 testing methodologies, replicates your network in action and support a wide range of protocols and applications, with realistic testing scenarios. By simulating real-world legitimate traffic, DDoS (Distributed Denial of Service), exploits, malware, and fuzzing, XproNS supports capacity, performance and security testing for network devices and solutions, cloud and virtual environments. XproNS provides the highest Layer 4-7 performance from 1Gbps to 400Gbps.

Test Scenarios

- Network Devices Performance Testing
- Industrial Control Protocol Testing
- IPSec and SSL VPN Testing
- Security Testing
- RFC 2544 Testing
- Cloud and Virtual Network Testing

Network Devices Performance Testing

XproNS provides performance and security testing on a variety of network devices including: NGFW (Next Generation Firewall), WAF (Web Application Firewall), DPI (Deep Packet Inspection), IDS/IPS, Load Balancer, DLP (Data Loss Prevention), Cache, Proxy, Reverse-Proxy, URL Filter, Content Filter, HTTP/HTTPS Accelerator, Anti-DDoS, Anti-Virus gateways, IPSec VPN Gateways, SSL VPN, and more. A single server (XproNS) can hit millions of connection establishment rate, 500 million level concurrent connections capacity as the highest performance.

Industrial Control Protocol Testing

XproNS can simulate the mainstream industrial control protocol stack, PLC and other device, conduct functional, performance and security testing on industrial control device in an easy and convenient manner and conduct function, performance and security defense capability testing on industrial control security devices.

Cryptographic Load Testing

XproNS provides extensive functional and performance testing for secure network communication, and user authentication including: IPSec (IKEv1 and IKEv2), HTTPS/TLS (SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3, all relevant and popular ciphers supported), DNS over TLS (DoT), SSL VPN and custom user imported traffic over TLS.

SSL VPN Testing

XproNS supports SSL VPN tunnel setup and data traffic throughput capacity testing over any vendor's SSL VPN device. Defining Logic in SSL VPN interaction process based on LUA script framework, to adapt to any private SSL VPN client access and authentication process of various SSL VPN device vendors.

RFC 2544 Testing

Based on dedicated FPGA network card, XproNS offers RFC 2544 test suite (Benchmarking Methodology for Network Interconnect Devices). Key tests include:

- Throughput
- Latency
- Frame loss
- Back-to-back frames

Security Testing

XproNS provides users an effective means to test with a database of tens of thousands of up-to-date attack, virus and malware scenarios. This allows you to mix attacks and applications to verify and analyze network security. You can add realistic hacker behavior with evasion techniques or encrypt attacks to test security solutions 'limitations.

- **DDoS**: Simulates a variety of volumetric, protocol, and application-layer DDoS attacks.
- **CVE based attack**: Simulates latest attack scenarios with CVE ID reference. The database includes 8,000+ attacks.
- **Virus/Malware**: Comprises a library of 18,000+ virus/malwares. Monthly virus/malware packages contain fast-changing virus/malware and botnet attacks.
- **MITRE ATT&CK™ framework**: Supports 12 tactics and hundreds of techniques in ATT&CK. Multiple ATT&CK scenario settings. Quickly select from attack tactics and techniques to validate specific vulnerability types.
- **Evasion techniques**: Supports multiple evasion techniques such as IP fragmentation, TCP segmentation, HTTP, FTP, etc.

- **Up to date**: The attack and virus database is continuously upgraded. Independent security research team tracks the latest cyber-attack techniques and attack methods, real reproduction of attack behavior. You also can upload malware sample files by yourselves and send the sample files through the specified protocol.
- **Fuzzing**: Scripts are written to modify protocol fields to malformed packets to validate integrity of different protocol stacks by sending malformed packets to the DUT.

Key Features

Features	XproNS
IP Version Supported	IPv4 and IPv6
Network Access Protocol	DHCP, IPoE, PPPoE, IPSec (IKEv1 and IKEv2), SSL VPN
Encapsulation Protocol	VxLAN, GRE, GTP-U, SRv6, L2TP, VLAN (802.1Q), 802.1 Q-in-Q
Transport Protocol	TCP, UDP, SCTP, MPTCP, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
Authentication	Diameter
Data Protocol	HTTP, HTTP/2, HTTPS, FTP (Active/Passive), DNS over TCP/UDP, DNS over TLS (DoT), TELNET, SMTP, POP3, IMAP4, ICMP, SSH, WebSocket, NETCONF, CUSP, XDMCP
Voice Protocol	SIP over TCP/UDP
Voice Codec Supported	G.711A, G.711U, G.723.1, G.726-16, G.726-24, G.726-32, G.726-40, G.728, G.729A, G.729AB
Video Protocol	Unicast Streaming RTSP/RTP, Flash Media Streaming using RTMP
Multicast Protocol	IGMPv2, MLDv1
Database Protocol	MySQL
File Access Protocol	CIFS (SMB)
Industrial Control Protocol	Modbus, OPCUA, Handle, LWM2M, CoAP, MQTT, IEC104, IEC61850_SMV, IEC61850_MMS, DNP3, Siemens S7, HART
Extended Protocols	Layer 2 Replay, Layer 3 Replay, Layer 7 Replay
Reporting	CSV and PDF format report
Automation	Restful API

Software Defined Tester

XproNS is a software defined tester and the dedicated appliance is NOT needed. Decoupling software and hardware to reduce cost investment. XproNS can be deployed on a universal X86 architecture hardware platform. You can purchase a new X86 server or reuse existing servers to install the XproNS software. You can upgrade your hardware combination (CPU, memory and network card) to achieve a flexible combination of performance and port density. XproNS also can be deployed in a range of private and public cloud computing environments based on technologies from VMware, KVM, OpenStack and Amazon Web Services.

Ordering Information

Licensing	Description
XproNS 20G	The total interface speed does not exceed 20G, e.g. 2x10G
XproNS 40G	The total interface speed does not exceed 40G, e.g. 4x10G
XproNS 80G	The total interface speed does not exceed 80G, e.g. 8x10G
XproNS 100G	The total interface speed does not exceed 100G, e.g. 2x10G & 2x40G
XproNS 200G	The total interface speed does not exceed 200G, e.g. 2x100G
XproNS 400G	The total interface speed does not exceed 400G, e.g. 4x100G
XproAttack	1 Year Subscription: including CVE based attack, exploits, Malware, DDoS, etc. Monthly update.
FPGA Card	for RFC2544 testing
QAT Card	Hardware acceleration card to improve encryption performance

Contact Us

Headquarter: Room 1606, Building 2, Beijing SDIC Fortune Plaza, No. 9 Guang'an Road, Fengtai District, Beijing

R&D Center: Room 803, Building A, Optics Valley World Trade Center, East Lake High-Tech Zone, Wuhan, Hubei Province

South China Marketing Center: Room 6306, Building 6, United Community, No. 379 Zhongshan Avenue Middle, Tianhe District, Guangzhou, Guangdong Province

East China Marketing Center: Room 2018, Shatian Building, No. 587 Changshou Road, Putuo District, Shanghai

Email: market@dotouch.com.cn