

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

XproNetworkSimulator (XproNS)**Комплексное решение для тестирования приложений и сетевой безопасности**

Решение Dotouch XproNetworkSimulator (XproNS) для тестирования приложений и безопасности предоставляет наиболее полный и проверенный в отрасли набор методик тестирования на уровнях L4-L7, воспроизводит работу реальной сети и поддерживает широкий спектр протоколов и приложений с реалистичными сценариями испытаний. Моделируя легитимный трафик реальных сетей, DDoS-атаки, эксплойты, вредоносное ПО и фаззинг, XproNS обеспечивает тестирование пропускной способности, производительности и безопасности сетевых устройств и решений, а также облачных и виртуальных сред. XproNS поддерживает высокую производительность на уровнях L4-L7 в диапазоне от 1 до 400 Гбит/с.

**Сценарии тестирования**

- Тестирование производительности сетевых устройств
- Тестирование промышленных протоколов управления
- Тестирование IPSec и SSL VPN
- Тестирование безопасности
- Тестирование по RFC 2544
- Тестирование облачных и виртуальных сетей

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Тестирование производительности сетевых устройств

XproNS обеспечивает тестирование производительности и безопасности различных сетевых устройств, включая межсетевые экраны нового поколения (NGFW), межсетевые экраны веб-приложений (WAF), системы глубокого анализа пакетов (DPI), IDS/IPS, балансировщики нагрузки, системы предотвращения утечек данных (DLP), кэширующие системы, прокси- и обратные прокси-серверы, фильтры URL-адресов и контента, ускорители HTTP/HTTPS, средства защиты от DDoS, антивирусные шлюзы, шлюзы IPsec VPN, SSL VPN и другие решения. Один сервер XproNS обеспечивает скорость установления соединений на уровне миллионов в секунду и поддерживает до 500 млн одновременных соединений в максимальной конфигурации.

Тестирование промышленных протоколов управления

XproNS может моделировать стеки распространённых промышленных протоколов управления, ПЛК и другие устройства, позволяя удобно проводить функциональное тестирование, проверку производительности и безопасности промышленного оборудования, а также оценивать функциональность, производительность и способность промышленных средств защиты противостоять атакам.

Нагрузочное тестирование криптографических функций

XproNS обеспечивает широкие возможности функционального и нагрузочного тестирования защищённых сетевых коммуникаций и аутентификации пользователей, включая IPsec (IKEv1 и IKEv2), HTTPS/TLS (SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 и TLSv1.3 с поддержкой всех актуальных распространённых наборов шифров), DNS over TLS (DoT), SSL VPN, а также импортированный пользователем трафик, передаваемый через TLS.

Тестирование SSL VPN

XproNS поддерживает проверку установления туннелей SSL VPN и пропускной способности трафика данных на устройствах SSL VPN любых производителей. Логика взаимодействия SSL VPN задаётся с помощью сценариев на базе Lua, что позволяет адаптироваться к частным процессам доступа и аутентификации клиентов SSL VPN различных производителей.

Тестирование по RFC 2544

На базе специализированной сетевой FPGA-карты XproNS предоставляет комплект тестов RFC 2544 - методику эталонного тестирования сетевых устройств. Основные испытания включают:

- Пропускная способность
- Задержка
- Потеря кадров
- Кадры back-to-back

Тестирование безопасности

XproNS предоставляет эффективные средства тестирования и базу из десятков тысяч актуальных сценариев атак, вирусов и вредоносного ПО. Это позволяет смешивать атаки и прикладной трафик для проверки и анализа сетевой безопасности. Для оценки ограничений средств защиты можно воспроизводить реалистичное поведение злоумышленников, применять техники уклонения от обнаружения и шифровать атаки.

- **DDoS:** моделирование различных объёмных DDoS-атак, атак на уровне протоколов и приложений.
- **Атаки на базе CVE:** моделирование актуальных сценариев атак со ссылками на идентификаторы CVE. База содержит более 8 000 атак.
- **Вирусы и вредоносное ПО:** библиотека из более чем 18 000 вирусов и образцов вредоносного ПО. Ежемесячные пакеты обновлений включают быстро меняющиеся угрозы и атаки ботнетов.
- **MITRE ATT&CK:** поддержка 12 тактик и сотен техник ATT&CK, а также нескольких вариантов настройки сценариев. Быстрый выбор тактик и техник позволяет проверять определённые типы уязвимостей.
- **Техники уклонения от обнаружения:** поддержка фрагментации IP, сегментации TCP и различных техник для HTTP, FTP и других протоколов.
- **Постоянное обновление:** базы атак и вирусов непрерывно обновляются. Независимая исследовательская группа отслеживает новейшие методы кибератак и реалистично воспроизводит поведение злоумышленников. Пользователь также может загружать собственные образцы вредоносных файлов и передавать их по выбранному протоколу.
- **Фаззинг:** сценарии изменяют поля протоколов и формируют некорректные пакеты, которые отправляются на тестируемое устройство для проверки устойчивости различных стеков протоколов.

Статистика и отчётность

XproNS предоставляет статистику в реальном времени по всем протоколам и формирует отчёты, которые можно экспортировать в форматы CSV и PDF.

Ключевые возможности

Характеристика	XproNS
Поддерживаемые версии IP	IPv4 и IPv6
Протоколы сетевого доступа	DHCP, IPoE, PPPoE, IPSec (IKEv1 и IKEv2), SSL VPN
Протоколы инкапсуляции	VxLAN, GRE, GTP-U, SRv6, L2TP, VLAN (802.1Q), 802.1 Q-in-Q
Транспортные протоколы	TCP, UDP, SCTP, MPTCP, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
Аутентификация	Diameter
Протоколы передачи данных	HTTP, HTTP/2, HTTPS, FTP (активный/пассивный режим), DNS over TCP/UDP, DNS over TLS (DoT), TELNET, SMTP, POP3, IMAP4, ICMP, SSH, WebSocket, NETCONF, CUSP, XDMCP

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Голосовые протоколы	SIP over TCP/UDP
Поддерживаемые голосовые кодеки	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
Видеопротокولات	Одноадресная потоковая передача RTSP/RTP, потоковая передача Flash Media по RTMP
Многоадресные протоколы	IGMPv2, MLDv1
Протоколы баз данных	MySQL
Протоколы доступа к файлам	CIFS (SMB)
Промышленные протоколы управления	Modbus, OPC UA, Handle, LWM2M, CoAP, MQTT, IEC104, IEC61850_SMV, IEC61850_MMS, DNP3, Siemens S7, HART
Расширенные протоколы	Повторное воспроизведение трафика уровня 2, уровня 3 и уровня 7
Отчётность	Отчёты в форматах CSV и PDF
Автоматизация	RESTful API

Программно-определяемый тестер

XproNS является программно-определяемым тестером и не требует специализированного аппаратного комплекса. Разделение программного и аппаратного обеспечения снижает капитальные затраты. XproNS можно развернуть на универсальной аппаратной платформе архитектуры x86: приобрести новый сервер x86 или повторно использовать имеющиеся серверы для установки программного обеспечения XproNS. Модернизация сочетания процессора, памяти и сетевой карты обеспечивает гибкую конфигурацию производительности и плотности портов. XproNS также можно развернуть в частных и публичных облачных средах на базе VMware, KVM, OpenStack и Amazon Web Services.

Информация для заказа

Лицензия	Описание
XproNS 20G	Суммарная скорость интерфейсов не превышает 20G, например 2 x 10G
XproNS 40G	Суммарная скорость интерфейсов не превышает 40G, например 4 x 10G
XproNS 80G	Суммарная скорость интерфейсов не превышает 80G, например 8 x 10G
XproNS 100G	Суммарная скорость интерфейсов не превышает 100G, например 2 x 10G и 2 x 40G
XproNS 200G	Суммарная скорость интерфейсов не превышает 200G, например 2 x 100G

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

XproNS 400G	Суммарная скорость интерфейсов не превышает 400G, например 4 x 100G
XproAttack	Годовая подписка, включающая атаки на базе CVE, эксплойты, вредоносное ПО, DDoS и другие сценарии. Ежемесячное обновление.
FPGA Card	FPGA-карта для тестирования по RFC 2544
QAT Card	Аппаратная карта ускорения для повышения производительности шифрования