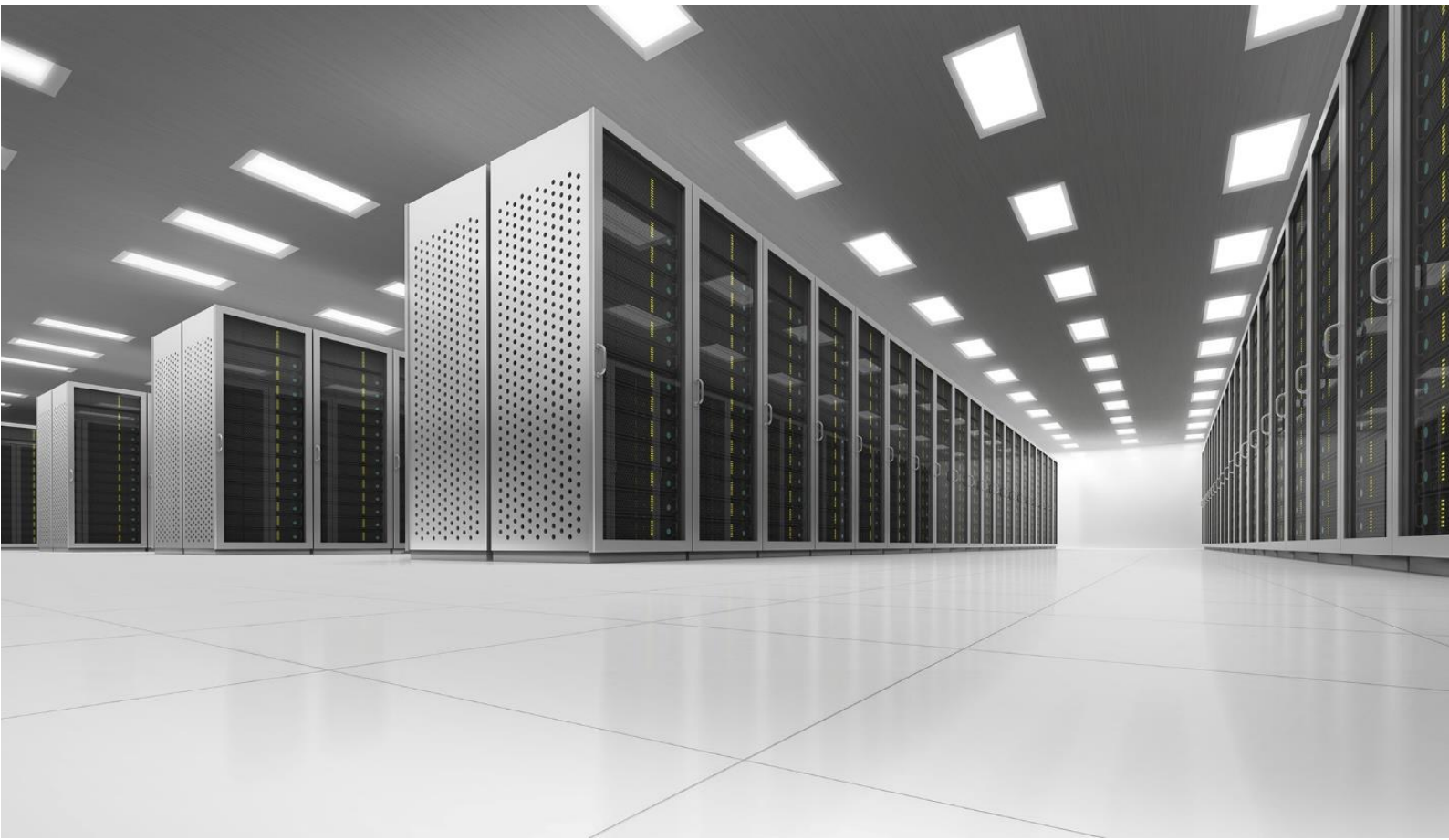
SPIRENT

cyberflood

(Спайрент Сайберфлад)

Лабораторный программно-аппаратный комплекс генерации трафика высокой интенсивности, кибератак и фаззинга сетевых и промышленных протоколов



CyberFlood: назначение комплекса

Программно-аппаратный комплекс CyberFlood (читается как «СайберФлад») предназначен генерации разнообразного *трафика приложений* поверх стека Ethernet/IP в условиях лаборатории[1] для стрессового тестирования информационных и телекоммуникационных систем и инфраструктуры.

Помимо экстремально высокой производительности генерируемого трафика, CyberFlood специально разработан как генератор широкого спектра хакерских атак L2-L7 уровней для тестирования устойчивости информационных систем и инфраструктуры (включая узлы транспортных сетей передачи данных) к киберугрозам

Что тестируется с помощью CyberFlood

С помощью CyberFlood выполняется нагрузочное тестирование таких устройств как:

- DPI
- IDS/IPS
- Антивирусные системы
- Балансировщики нагрузки
- Межсетевые экраны
- Серверы приложений
- Киберустойчивость критической инфраструктуры
- Устойчивость к атакам новых технологических решений на основе интернета вещей (IoT), роботизированных систем и многое другое

Цели тестирования:

- выбор и подтверждение работоспособности разработанных изделий (PoC);
- выбор поставщиков телекоммуникационного оборудования (бэнчмаркинг),
- настройка периметров информационной защиты от киберугроз;
- сертификация оборудования;
- образовательные цели.

Кто использует такое тестирование?

> Разработчики информационных систем и оборудования, операторы связи, операторы ЦОДов, государственные учреждения, банки, системные интеграторы, сертифицирующие организации, профильные ВУЗы.

[1] Лабораторное нагрузочное тестирование подразумевает отключение от публичных и корпоративных сетей

Состав комплекса CyberFlood

Комплекс состоит из нескольких ключевых аппаратных, программных и подписных компонентов.

❶ Платформа генерации трафика

В настоящее время предлагается несколько типов платформ, на которых запускается CyberFlood:

ТИП ПЛАТФОРМЫ			
Аппаратная			**Виртуальная**
Spirent C1	CF20	C100	CyberFlood Virtual
			
Портативный прибор начального уровня с интерфейсами 1/10Gb	Платформа с возможностью генерации трафика на скоростях от 1Гб/с до 100Гб/с	Высокопроизводительная платформа генерации трафика на скоростях до N x 100 Гбит/с (multi rate – все скорости кроме 1GbE)	Виртуальный генератор трафика

Генератор трафика C100 в конфигурации 4x10G и 16x1G

Для выполнения тестов пользователи подключаются к платформе удаленно по локальной или глобальной сети Ethernet. Для работы с генератором трафика пользователю достаточно только браузера.

❷ Набор опций (лицензий) тестирования

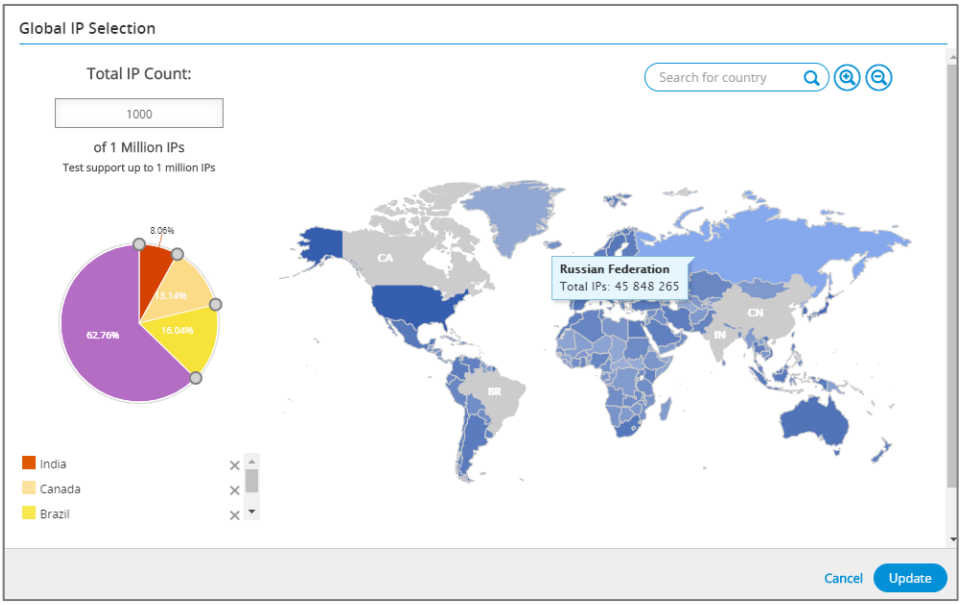
Описание
Тестирование киберустойчивости информационных систем
Генерация массированных DDoS-атак
Нагрузочное тестирование DNS серверов
Генерация мультипротокольного смешанного трафика
Методология тестирования на максимальное количество открытых HTTP соединений
Методология тестирования максимальной пропускной способности по протоколу HTTP
Опция воспроизведения пользовательского трафика
Генерация атак DDoS протокольного уровня
Генерация атак DDoS прикладного уровня
Опции фаззинга различных протоколов

Лицензии могут быть как постоянные, так и подписные.

❸ Подписки на обновление баз данных

Данные опции выполняют одну из ключевых ролей в работе программно-аппаратного комплекса, поскольку позволяют поддерживать базы знаний по кибератакам в актуальном состоянии. Обновление базы прикладного трафика позволяет постоянно добавлять новые разновидности трафика сетевых приложений и их версий. В составе есть четыре основные базы знаний, которые требуют периодической актуализации:

1. База атак генерации
2. База вредоносного контента (malware)
3. База трафика приложений
4. База глобальной IP-адресации и подсетей в соответствии с разделением адресного пространства IANA (Internet Assigned Numbers Authority). Это позволяет генерировать географически-окрашенный трафик и кибератаки с помощью простой визуальной настройки:



Пример настройки генерации географически-окрашенного трафика в интерфейсе CyberFlood

Продолжительность стандартной подписки составляет один, два или три года. По истечении срока подписки, она может быть продлена.

❹ Атаки типа Zero-day. Генерация атак с применением технологии Фаззинг по стекам протоколов

Fuzzing (произносится как «фаззинг») – разновидность хакерских атак, которая подразумевает отправку нестандартных запросов на серверы или элементы транспортной сети с целью получения нестандартного отклика оборудования или систем. Такое воздействие может привести к нестандартному функционированию оборудования, что используется как первый этап многоступенчатых атак или поиск недокументированных возможностей сетевого оборудования (бэкдоры) и программ. В рамках фаззинга нестандартные запросы могут отправляться не только на прикладном уровне (например, в адресной строке браузера по протоколу http), но и на других уровнях OSI и протоколах, в том числе транспортных. В этом случае объектом атаки могут становится не только прикладные серверы, но транспортные маршрутизаторы, BRASы, CG-NAT и другие объекты опорной сети операторов связи.

CyberFlood генерирует трафик различных протоколов которые подвергаются мутации с помощью фаззинга. К таким протоколам относятся IP, ARP, LACP, 802.x, BFD, DGP, DHCP, RADIUS, ZIGBEE, CIFS, DNS, GTP, H.248, HTTP(s) и многие другие.

❺ Доступ к технической поддержке

Техническая поддержка является важной частью обеспечения нормального жизненного цикла такого продукта как CyberFlood. Техническая поддержка подразумевает доступ на web-портал поддержки пользователей Customer Service Center.

Опция Техподдержки открывается на определенный период времени – один, два или три года.

Возможности и преимущества CyberFlood

Тестирование киберустойчивости IT и телекоммуникационных систем

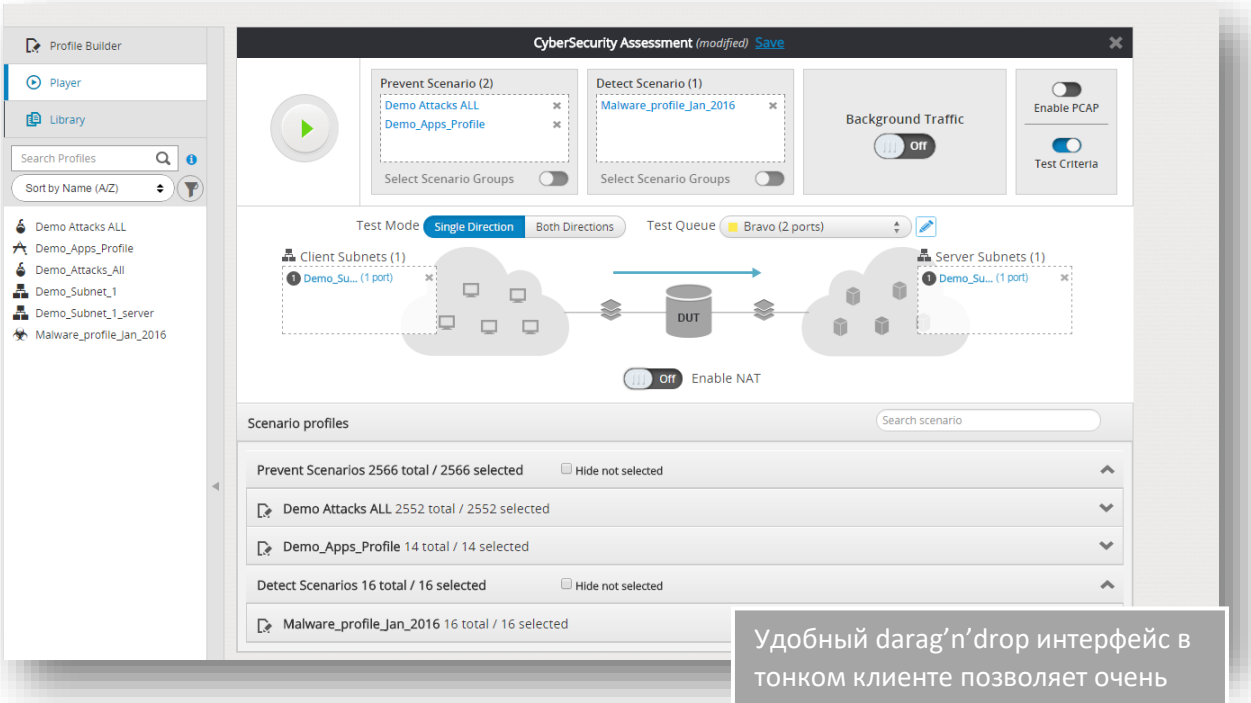
- Тестирование известных уязвимостей с помощью базы из более чем 15000 атак
- Генерация атак нулевого дня с
- Генерация фаззинга различных протоколов для поиска уязвимостей критической инфраструктуры и сетевых приложений
- Оценка возможности детектирования вредоносного кода (Malware) на самых актуальных сигнатурах и бинарном коде. Речь идёт о технологиях атак как Worms, Virus, Trojan, Spyware, Root Kits, File Infector, Adware, Bots, Backdoors
- Эмуляция зараженных хостов
- DDoS на линейной скорости физического интерфейса Ethernet, включая генерацию массированных DDoS-атак, DDoS по протоколам (на объекты сетевой инфраструктуры) и DDoS-атаки на прикладном уровне. Примеры атак DDoS, которые генерирует CyberFlood: ICMP, UDP, Spoofed IP, Malformed IP/UDP/ICMP, Ping of death, Synflood, Smurf, HTTP GET floods, SIP Invite floods и многие другие варианты.

Максимальная реалистичность генерируемого трафика

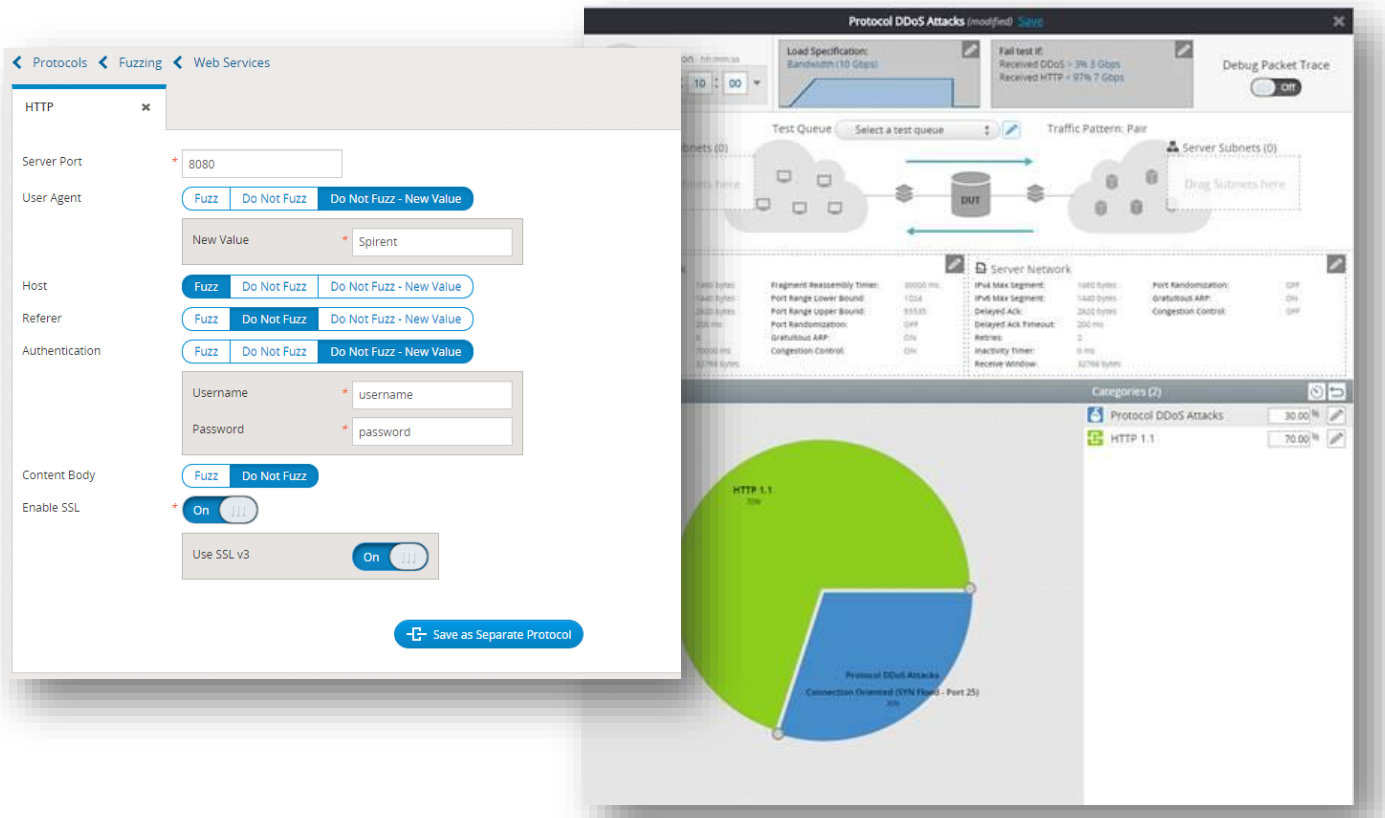
- Генерация смешанных профилей трафика, как на реальных сетях
- Генерации сценариев сетевых приложений из более чем 10000 приложений
- Генерация простых протоколов с возможностями их параметризации

Высокая производительность генерации трафика

- Генерация stateful-трафика на линейных скоростях физических интерфейсов (1-100G – в зависимости от типа) Ethernet, установленных в аппаратном шасси Spirent C100
- 3,5 миллиона новых TCP-соединений в секунду
- 150 миллионов открытых соединений

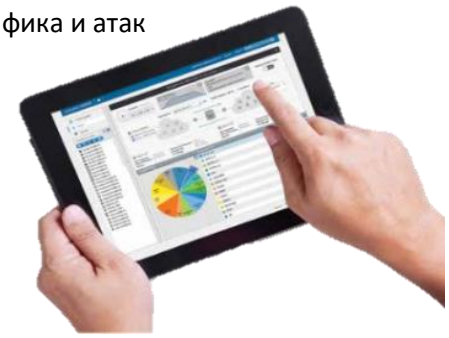


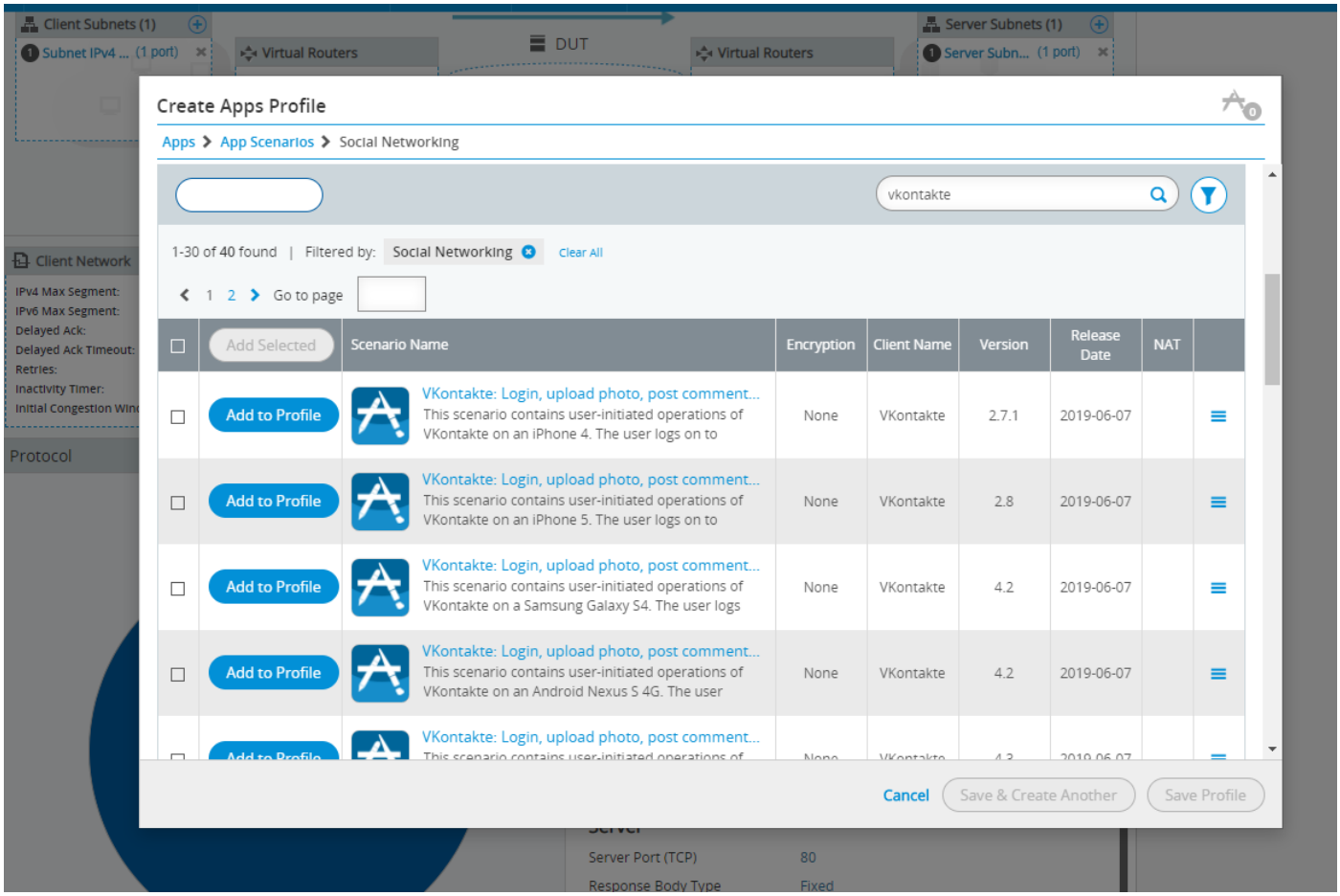
Удобный darag’n’drop интерфейс в тонком клиенте позволяет очень быстро настроить любой, даже сложный тестовый сценарий прямо в браузере



Актуальность и удобство использования

- Периодически обновляемые базы данных генерации трафика и атак
- Самые актуальные приложения и кибератаки
- Автоматическое и быстрое обновление контента
- Простой и понятный интерфейс пользователя с максимальным использованием графических возможностей браузера
- Встроенные методики тестирования
- REST API





О компании Spirent Communications

Компания SPIRENT является лидером в области лабораторных решений по тестированию телекоммуникационного оборудования. Экспертиза компании в области стрессового тестирования и линейка продуктов распространяется на следующие сегменты:

- Широкополосные сети: MPLS, DOCSIS 3.0, DSL, 10/100/100 Ethernet, 40/100 GbE и IP
- Конвергентные технологии: VoIP, IP VPNs, IPTV
- Сети NGN: Ipv6
- Беспроводные технологии связи: HSPA+, LTE, 3G/4G, CDMA, UMTS, MIMO & Advanced Antenna Technique, системы позиционирования
- Корпоративные сети: облачные вычислительные системы, виртуализация, нагрузочное тестирование, производительность сетевых устройств, тестирование безопасности сетей и приложений

Информация о **CyberFlood** на сайте Spirent Communications