

ПЛАТФОРМА ДЛЯ ТЕСТИРОВАНИЯ ПРОИЗВОДИТЕЛЬНОСТИ УСТРОЙСТВ СЕТИ И БЕЗОПАСНОСТИ

BreakingPoint – решение для тестирования приложений и уровня безопасности, которое позволит проверять стабильность, точность и качество работы сетей и сетевых устройств.



В современных условиях компании полагаются на самые разнообразные решения для защиты своих сетей от кибератак и пиковых нагрузок сети. С увеличением числа приложений усложняется инфраструктура безопасности, что в результате приводит к появлению хаотичного набора решений безопасности, работу которых трудно контролировать и масштабировать. Хуже того, возникающее усложнение системных взаимодействий представляет серьезную угрозу безопасности и устойчивости сети.

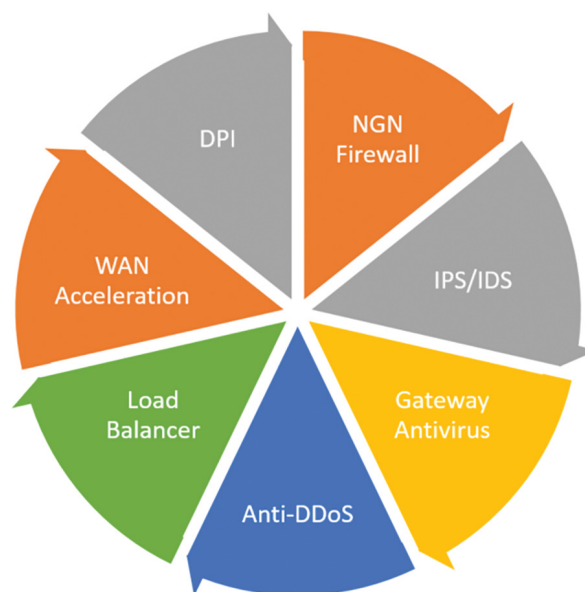
Поэтому предприятиям требуется решение для тестирования приложений и уровня безопасности, которое позволит проверять стабильность, точность и качество работы сетей и сетевых устройств.

С помощью имитации реального трафика, DDoS атак, эксплойтов, вредоносных программ, а также фаззинга платформа BreakingPoint позволяет производить тестирование инфраструктуры, снижает риск деградации сети почти на 80% и повышает готовность к атакам почти на 70%.

Проверка конкретных настроек или конфигурации безопасности на пригодность к защите от атак осуществляется платформой BreakingPoint с помощью имитации легитимного и вредоносного трафика. Это позволяет подтвердить надежность защиты и оптимизировать сеть согласно наиболее реалистичным условиям.

BreakingPoint позволяет осуществлять тестирование:

- Служб обнаружения и предотвращения вторжений (IDS/IPS).
- Шлюзовых антивирусов.
- Межсетевых экранов новейшего поколения.
- Средств защиты веб-приложений (WAF).
- Фильтров URL-адресов.
- Средств защиты от DDoS-атак.
- Прокси/кэша.
- Контент-фильтров.
- WAN-оптимизаторов.
- Углубленной проверки пакетов (DPI).
- Средств балансировки сетевой нагрузки / контроллеров доставки приложений.
- Анализаторов сети.
- Систем хранения данных.
- IPsec VPN.
- Углубленной проверки пакетов SSL, SSL-прокси, SSL-ускорения.



Основные возможности

- Имитация более 300 реальных приложений.
- Настройка и изменение любых протоколов, включая исходные данные.
- Создание набора протоколов на высокой скорости с реалистичным объемом.
- Стресс-тестирование инфраструктуры сети с использованием более 37 000 типов атак, вредоносных программ, ботнетов и методов обхода средств защиты.
- Эмуляция сложных, масштабных DDoS атак и атак с использованием ботнетов для выявления скрытых недостатков.
- Измерение производительности сетевых устройств и устройств безопасности.
- Возможности по обучению персонала путем моделирования реалистичного кибер-полигона / среды обучения.
- Проверка эффективности и отказоустойчивости сетей провайдера с использованием 3G/4G/LTE.
- Обновление базы данных приложений и атак два раза в месяц с исследовательской командой Application and Tread Intelligence (ATI).
- Использование программы TrafficREWIND для копирования параметров трафика непосредственно из вашей продуктивной сети для последующего использования при тестировании.

Для выпуска обновлений BreakingPoint команда исследователей ATI использует передовые методы наблюдения и исследований для поиска, сбора и быстрого обновления информации. Обновления выпускаются каждые две недели в течение уже более 10 лет, и библиотека пакета услуг ATI включает более 37 000 типов атак (эксплойтов, вредоносных программ, DDoS атак и т. д.), более 360 популярных приложений и более 2000 готовых к запуску тестов.

Кроме того, пакет услуг АТІ обеспечивает:

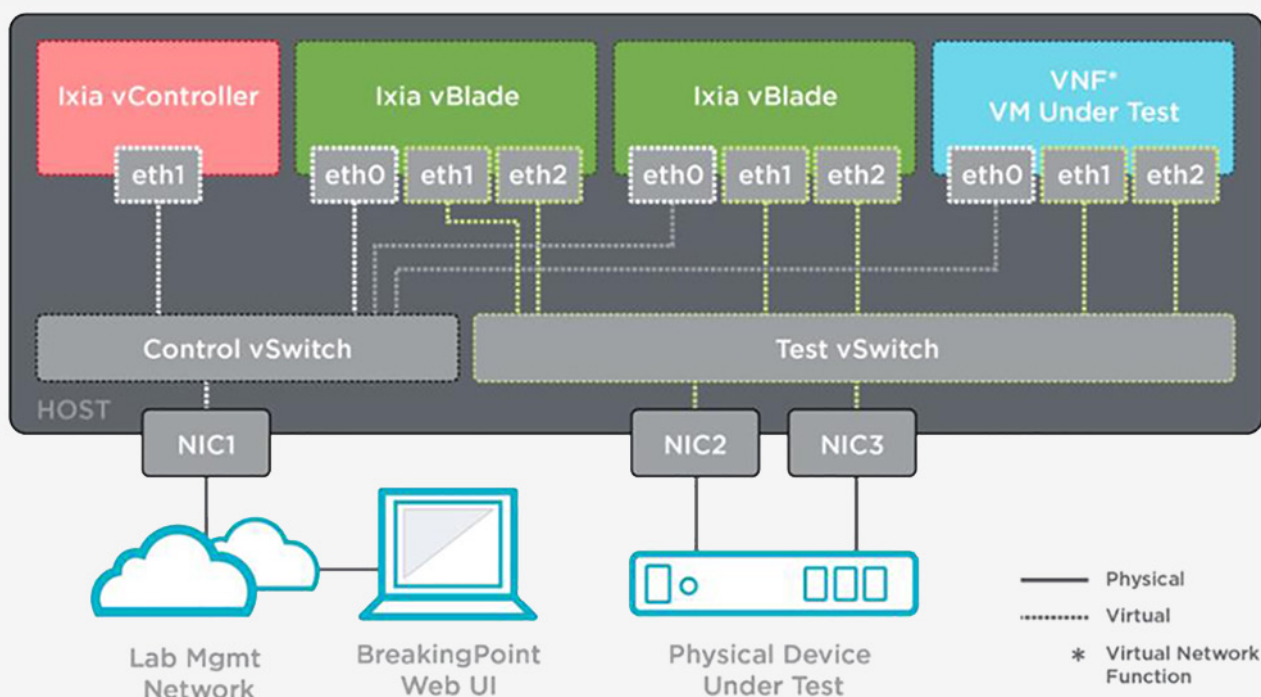
- Добавление в базу данных BreakingPoint новейших приложений и атак без необходимости обновления прошивки или ОС.
- Оповещение пользователей о последних событиях кибермира благодаря добавлению популярных приложений и обновлению уже существующих.
- Ежемесячное обновление базы данных вирусов и вредоносных программ, содержащее самые последние вирусы и атаки с использованием ботнетов.
- Хорошо изученные, реальные наборы приложений, которые позволяют эмулировать модели трафика для разнообразных демографических и бизнес условий.

Варианты конфигурации

1. [Оборудование BreakingPoint](#)

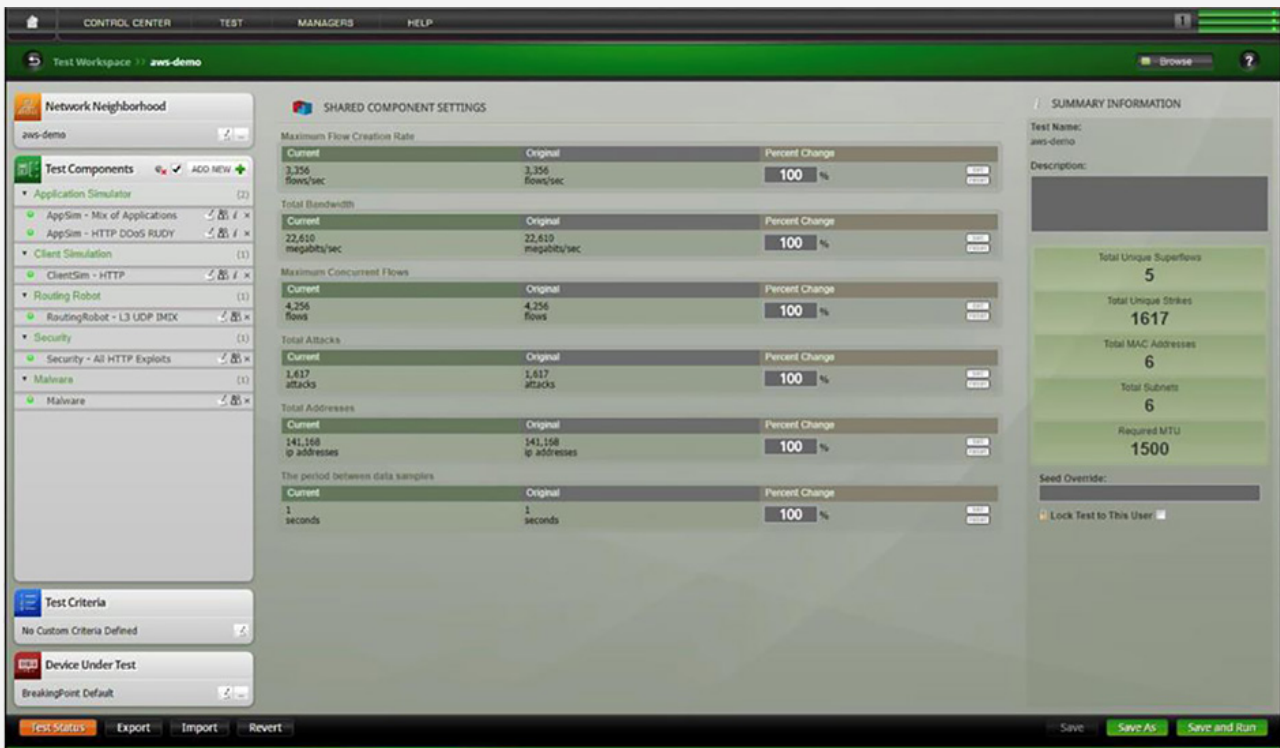
			
Metric	PERFECTSTORM ONE FUSION 8X10G/2X40G	PERFECTSTORM FUSION 8X10G/2X40G	CLOUDSTORM FUSION 2X100G
App Throughput	80Gbps	80Gbps	200Gps
TCP Connections per Second	1.45 Million	1.45 Million	3.5 Million
App Concurrent Flows	60 Million	60 Million	120 Million
SSL Bandwidth	20Gbps	20Gbps	65Gbps

2. [BreakingPoint VE](#)



BreakingPoint VE deployment for both virtual and physical device tests

3. [Облако BreakingPoint](#) и [решение BreakingPoint AWS](#)



BreakingPoint GUI configured with an enterprise cloud workload



Группа компаний БАКОТЕК – официальный дистрибьютор Ixia в Украине, Республике Беларусь, Азербайджане, Грузии, Армении, Казахстане, Кыргызстане, Молдове, Таджикистане, Туркменистане и Узбекистане.
www.bakotech.com, ixia@bakotech.com, +38 044 273 33 33.

IXIA WORLDWIDE
26601 W. AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942
(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805
www.ixiacom.com

IXIA EUROPE
CLARION HOUSE, NORREYS
DRIVE MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127