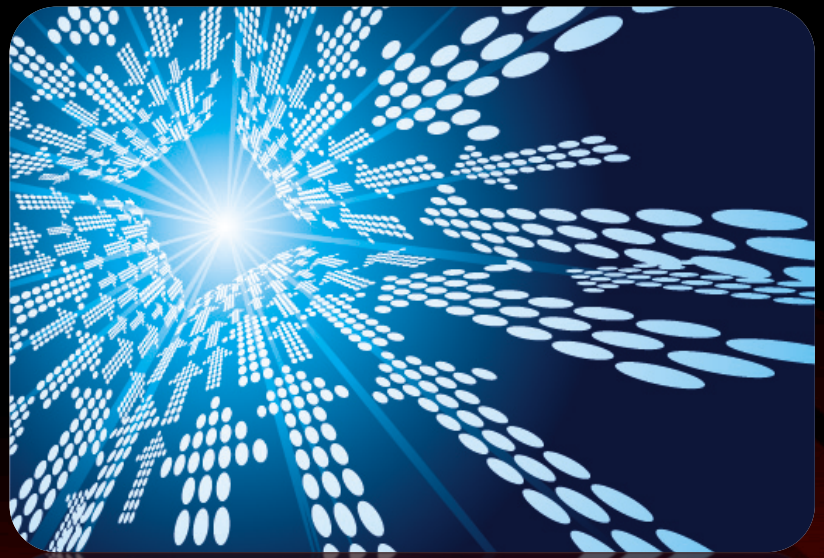
Высокоэффективное тестирование средств обеспечения кибербезопасности

Драйверы роста отрасли



- Виртуализация сетевой и компьютерной инфраструктур
- Все более широкое использование мобильных платформ в бизнесе
- Перемещение приложений и сервисов в облако
- Вопросы безопасности выходят на передний план в связи с необходимостью защищать облако, мобильные устройства и ЦОД

Высокоэффективная доставка приложений

Идентификация

По приложениям, а не по портам и протоколам
По пользователям и группам, а не по IP
Путем анализа контента, а не по имени файла

Категоризация

По приложениям
По типу приложений
По получателям
По контенту
По пользователям и группам

Контроль

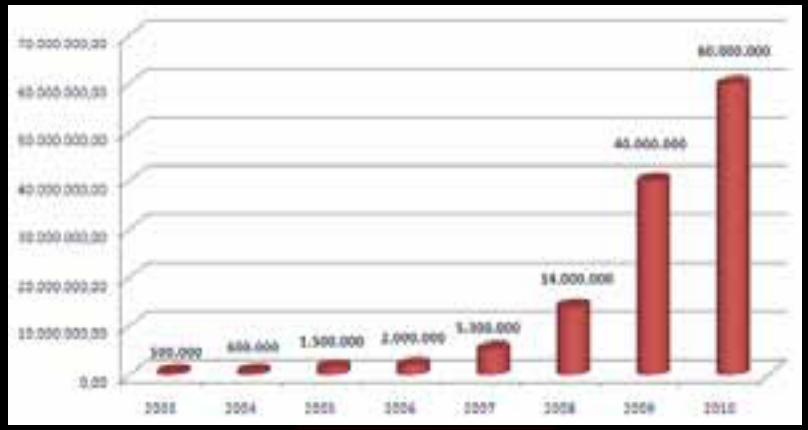
Приоритизация приложений по правилам политики
Управление приложениями по правилам политики
Блокировка приложений по правилам политики
Обнаружение и блокировка вредоносного ПО
Обнаружение и предотвращение попыток вторжения

Обеспечение безопасности при доставке приложений

Источник: SONICWALL

Взрывной рост числа угроз информационной безопасности

- Кибербезопасность: угрозы продолжают эволюционировать
  - В 2010 г. появились 20 млн новых вариантов вредоносного ПО
  - Из всех существующих вредоносных программ 34% появились в 2010 г.
  - **Ежедневно** подвергаются атакам 340 тыс. компьютеров
  - До 30% эксплойтов устанавливают кейлоггеры и трояны, которые **не используют жесткий диск**



- **Обход** применяется почти во всех случаях
  - Кодировка Base64 (single pad, double pad и др.), кодировка UTF-32 (LE и BE) и др.
- Хакерство превращается из хобби в выгодный бизнес
  - 78% реализованных угроз информационной безопасности экспортировали пользовательские данные
  - В 70% случаев атакам подвергались банки
  - В 2010 г. объем киберпреступной экономики составил более триллиона долларов

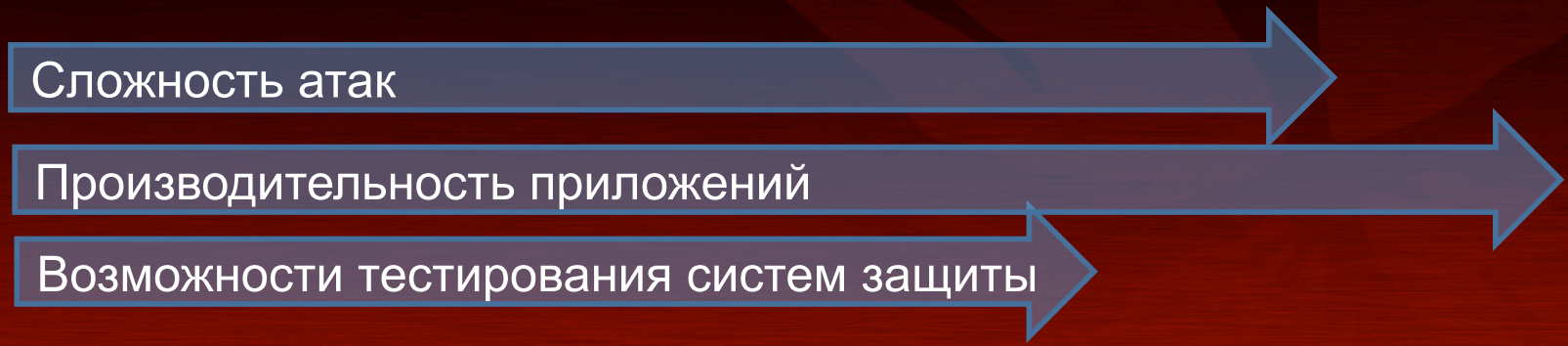
Эволюция угроз

Эволюция угроз

- Бэкдоры
- DoS-атаки
- DDoS-атаки
- Переполнение буфера
- Внедрение кода
- Вредоносный контент

Защитные технологии

- Обнаружение вторжений
- Предотвращение вторжений
- Объединенный контроль угроз



Распространение ботнета Zeus

- В феврале 2010 г. ботнет Zeus контролировал ~75 тыс. компьютеров в более чем 2400 организациях
- За четыре недели с помощью ПО Zeus было украдено более 68 тыс. учетных записей
- Самый большой единый ботнет, управляемый с помощью платформы Zeus, состоял из 600 тыс. зараженных компьютеров

Места расположения командных центров ZBot/Zeus (данные ZeuS Tracker)

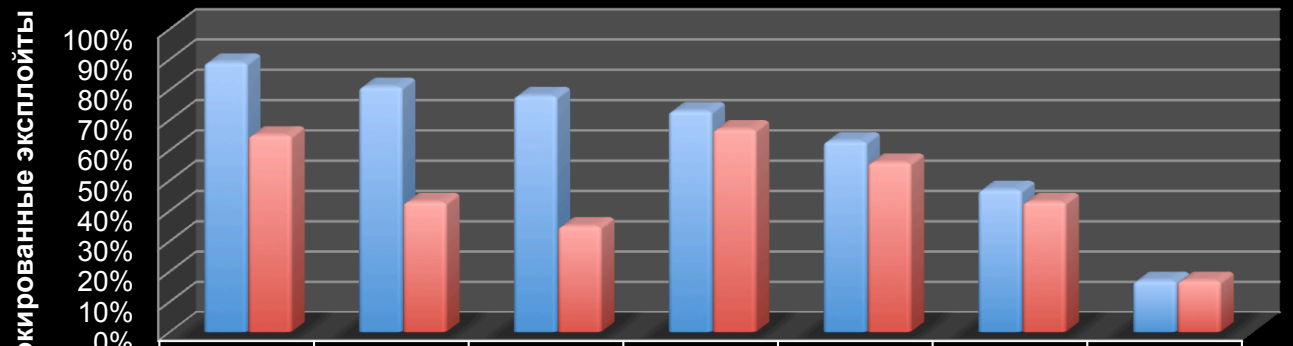
Вред от кибератак на сети

- Потеря данных
- Потеря времени
- Финансовые потери
- Отказ в обслуживании
- Судебное преследование
- Потеря репутации
- Проблемы в работе иранских ядерных объектов в Бушере

Эффективность: режимы по умолчанию против настройки

- Нет ширпотребу: разница в 72% между 89% и 17%
- Используемых по умолчанию правил политики безопасности и параметров конфигурации не достаточно

Доля блокированных эксплойтов: по умолчанию против настройки

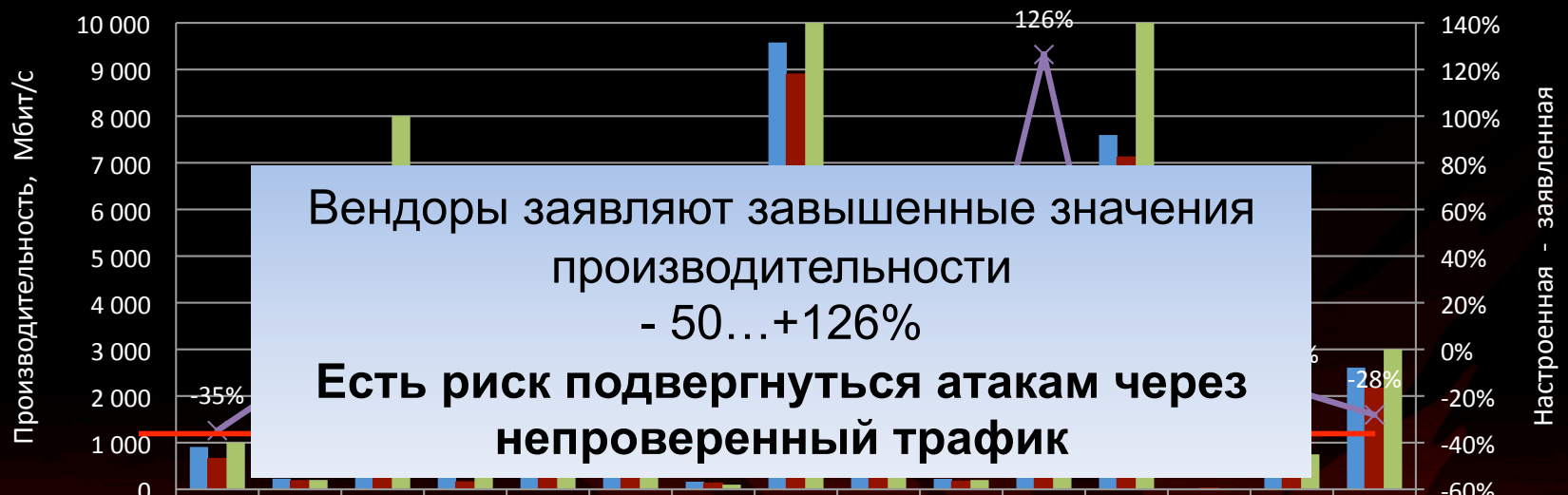


	Product A	Product B	Product C	Product D	Product E	Product F	Product G
Tuned	89%	81%	78%	73%	63%	47%	17%
Default	65%	43%	35%	67%	56%	43%	17%

Источник NSS Labs

Значения производительности сильно разнятся: не доверяйте утверждениям типа «работает на полной скорости канала»

Реальная производительность по сравнению с заявленной



Вендоры заявляют завышенные значения производительности
- 50…+126%
Есть риск подвергнуться атакам через непроверенный трафик

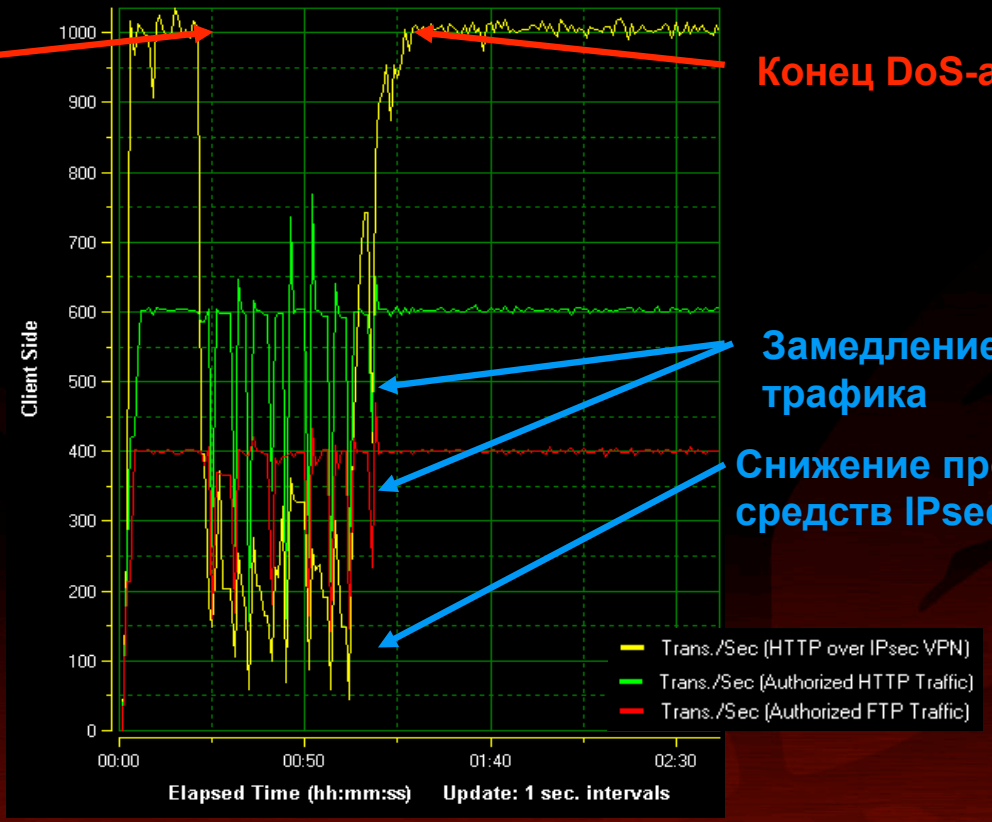
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Default	907	228	6 933	326	411	1 018	163	9 580	1 904	224	833	7 596	17	740	2 609
Tuned	652	178	6 512	151	331	698	125	8 893	1 807	162	793	7 116	16	620	2 158
Claimed	1 000	200	8 000	300	500	800	100	10 000	2 000	200	350	10 000	20	750	3 000
Delta %	-35%	-11%	-19%	-50%	-34%	-13%	25%	-11%	-10%	-19%	126%	-29%	-18%	-17%	-28%

Источник: NSS Labs

Влияние DDoS-атаки на производительность

Начало DoS-атаки

Конец DoS-атаки



Замедление клиентского трафика

Снижение производительности средств IPsec

Результаты тестирования межсетевого экрана

DDoS-атаки против серверов Wikileaks порождали трафик интенсивностью более 10 Гбит/с

Тестирование устройств защиты сетей

- **Эффективность защиты**
  - Способность обнаруживать и блокировать вредоносный трафик
  - Эффективность = число блокированных атак/число попыток атаковать

- **Точность обнаружения**
  - Число ложноположительных результатов
  - Блокирование легитимного трафика = отказу в обслуживании
- **Масштабируемость и производительность**
  - Производительность при доставке приложений
  - Влияние на QoE при отражении атак
  - Противодействие многочисленным интенсивным атакам

- **Доступность**
  - Доступность = 100% x время работы/(время работы + время простоя)

Представление IxLoad-Attack

Возможности IxLoad-Attack

Тестирование на уязвимость и распространение вредоносного ПО

- Более 6000 уникальных атак
- Различные методики обхода средств защ
- Двунаправленные атаки
- Частые обновления описаний атак
- Атаки через туннель IPsec

Атаки **DoS** и **DDoS**

- Имитация этих атак на линейных скоростях GE and 10GE
- 26 DDoS-атак L2/L4

Тестирование производительности

- Работает с ПО IxLoad и высокопроизводительными средствами генерации трафика
- TCP- и UDP-трафик

Проверка эффективности средств защиты под нагрузкой

- Вставка атак в легитимный трафик
- Измерение показателей QoE
- Внедрение вредоносного ПО через туннель IPsec

Тестирование предотвращения утечки данных

- Передача конфиденциальных данных
- Email, HTTP, FTP, IM
- ZIP-архив, PDF, XLS, DOC

Базы данных вредоносного ПО и вирусов в составе IxLoad-Attack

Стратегическое партнерство с ведущими поставщиками антивирусных решений

200 тыс. образцов вредоносных программ

- Самая полная и современная коллекция вредоносного ПО
- Кейлоггеры, бэкдоры, руткиты, трояны-вымогатели, перезаписывающие вирусы и др.
- Приносящие наибольший вред программы, такие как Conficker и Stuxnet
- Осуществление атак с использованием вредоносного ПО посредством HTTP, FTP, IMAP и других видов сетевого транспорта
- Коды, встроенные в файлы .pdf, .doc, .ppt, .xls и видеофайлы
- Двоичные исполняемые файлы и сценарии

Самая полная в отрасли имитация действий вредоносного ПО для тестирования:

- отдельных сетевых устройств,
- виртуализированных ЦОДов,
- облачных инфраструктур,
- мобильных и проводных сетей

Конкурентные преимущества решения Ixia

№1 по производительности и масштабируемости

- Высочайшая плотность портов на рынке
- Имитация (на линейной скорости) атак DoS/DDoS для портов GE и 10GE
- Имитация (на линейной скорости) IPsec VPN, исходящих из портов GE и 10GE

Самый полный охват атак

- Более 6000 уникальных атак
- Миллион модификаций атак, реализуемых с помощью методик обхода средств обеспечения кибербезопасности
- Самый полный охват решений крупнейших производителей, включая Microsoft
- Атаки, инициируемые взломщиками и внутренними пользователями

Результаты исследований в области информационной безопасности от двух пионеров отрасли

- TELUS Security Labs и Karalon

Смесь высокоскоростного трафика различных приложений

- Полнофункциональный прикладной уровень, охватывающий протоколы передачи голоса, данных и видео
- Широкие возможности измерения и анализа показателей Quality of Experience

Новаторские продукты Ixia для всестороннего тестирования приложений и средств обеспечения кибербезопасности

Представление семейства Xcellon-Ultra

Xcellon-Ultra™ NP*

Масштабируемое тестирование производительности на уровнях 2–7 (модуль для шасси XM)

- Проверенная архитектура NP
- Хорошая масштабируемость при работе на уровнях 2–7

Xcellon-Ultra™ XT

Сверхвысокая производительность при тестировании с использованием трафика приложений

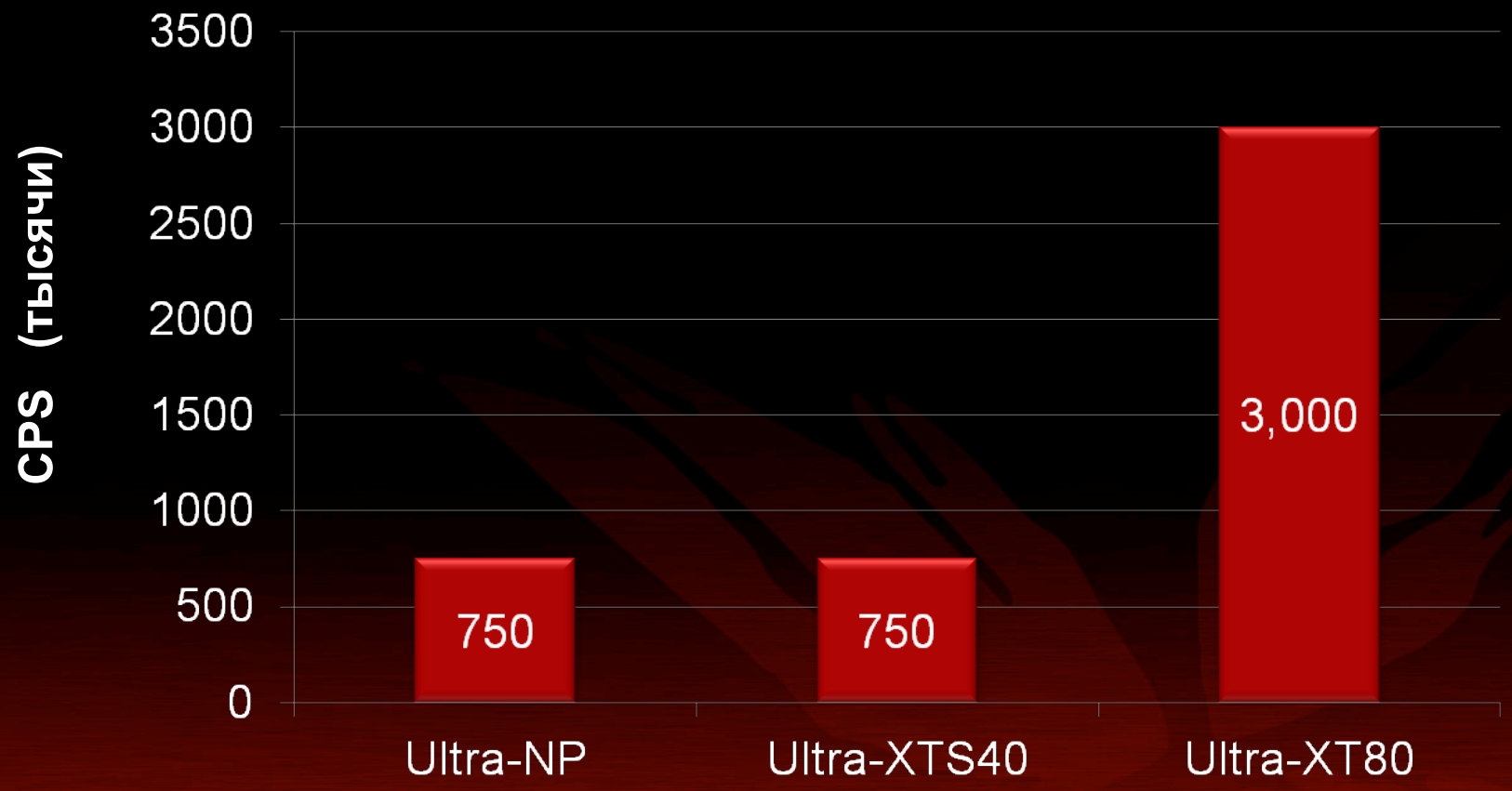
- Высочайшая плотность портов 10G
- Высочайшая производительность при работе с SSL

Xcellon-Ultra™ XTS

Сверхвысокая производительность при тестировании с использованием IPsec-трафика

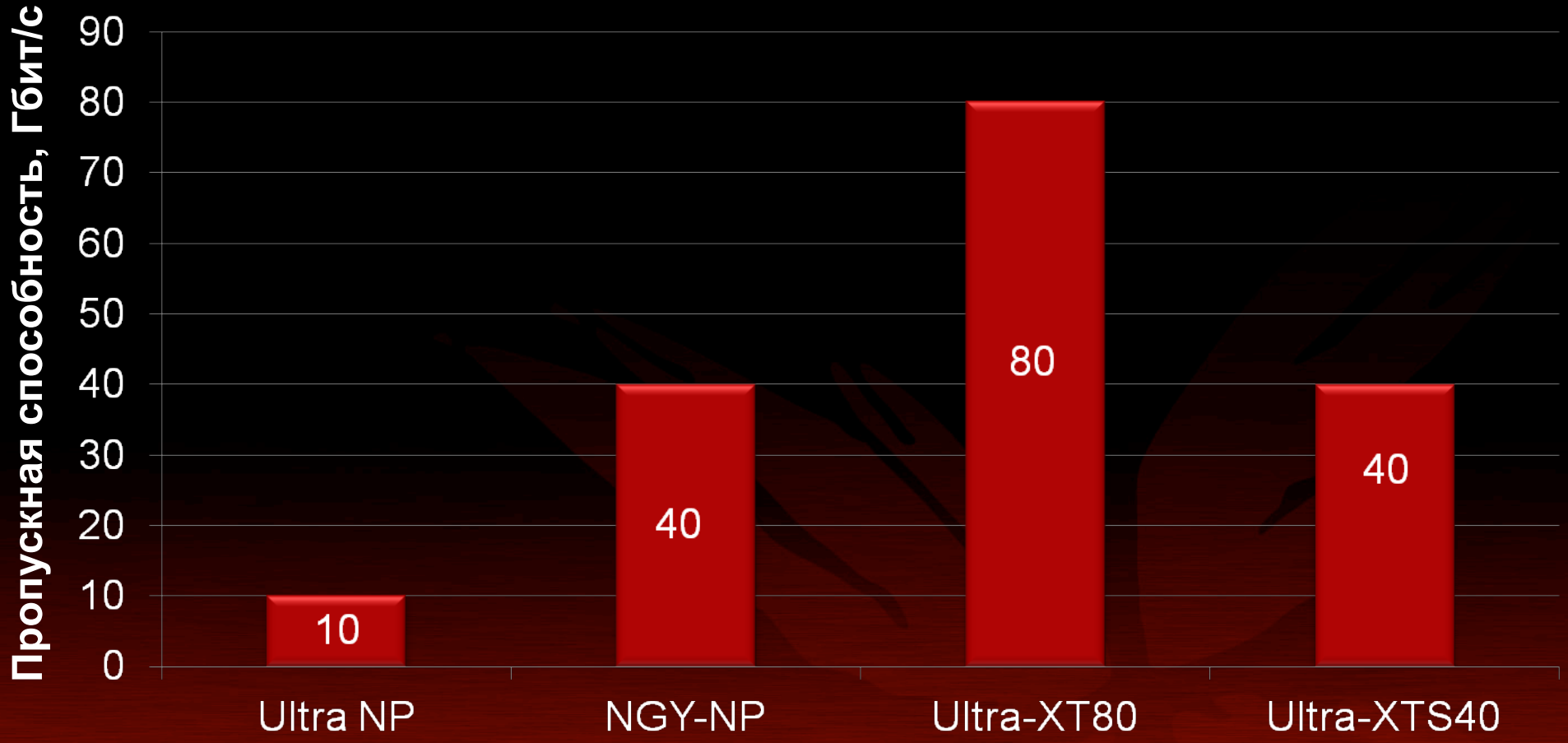
- Высочайшие скорость передачи IPsec-трафика и интенсивность образования туннелей

Число соединений в секунду (CPS)



*Все показатели относятся к паре модулей или устройств

Пропускная способность



*Все показатели относятся к паре модулей или устройств

Виды тестирования устройств защиты сетей с помощью решения Ixia

Тест №1: проверка эффективности и точности работы защитных устройств

Цель:

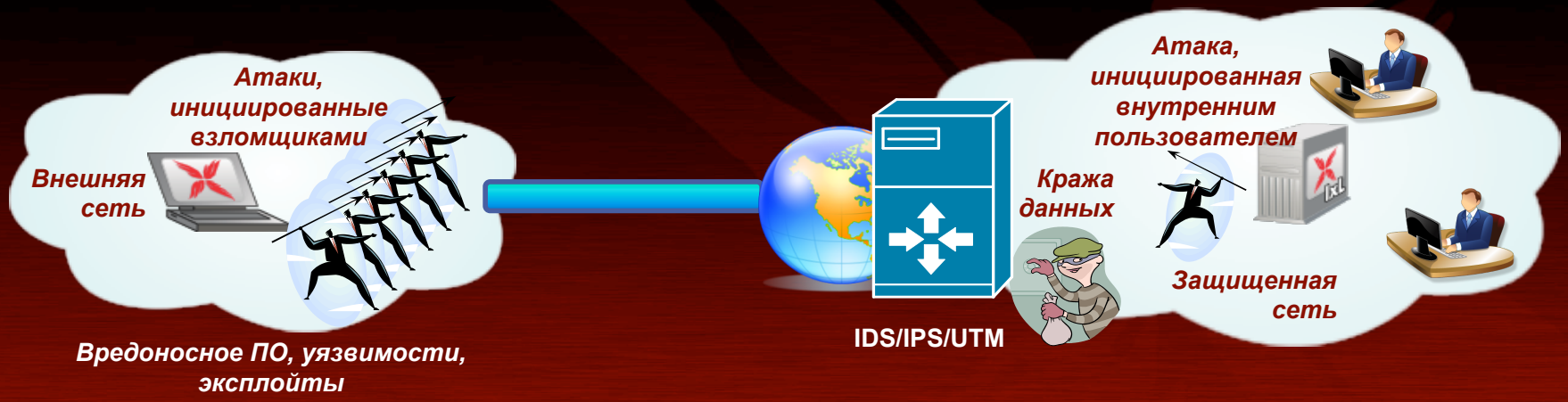
Проверить способность тестируемого устройства обнаруживать, протоколировать и блокировать угрозы. Оценить его эффективность и точность при наличии и отсутствии фонового трафика.

Тестируемые устройства:

Устройства IDS/IPS или UTM, обнаруживающие и блокирующие атаки; DLP-устройства

Метод тестирования:

Подключить тестируемое устройство к группе клиент-серверных портов.
Последовательно инициировать нежелательный трафик без фонового трафика.
Повторить это при наличии реалистичной смеси разных видов фонового трафика.



Тест №2: тестирование производительности защитных устройств при осуществлении атак

Цель:

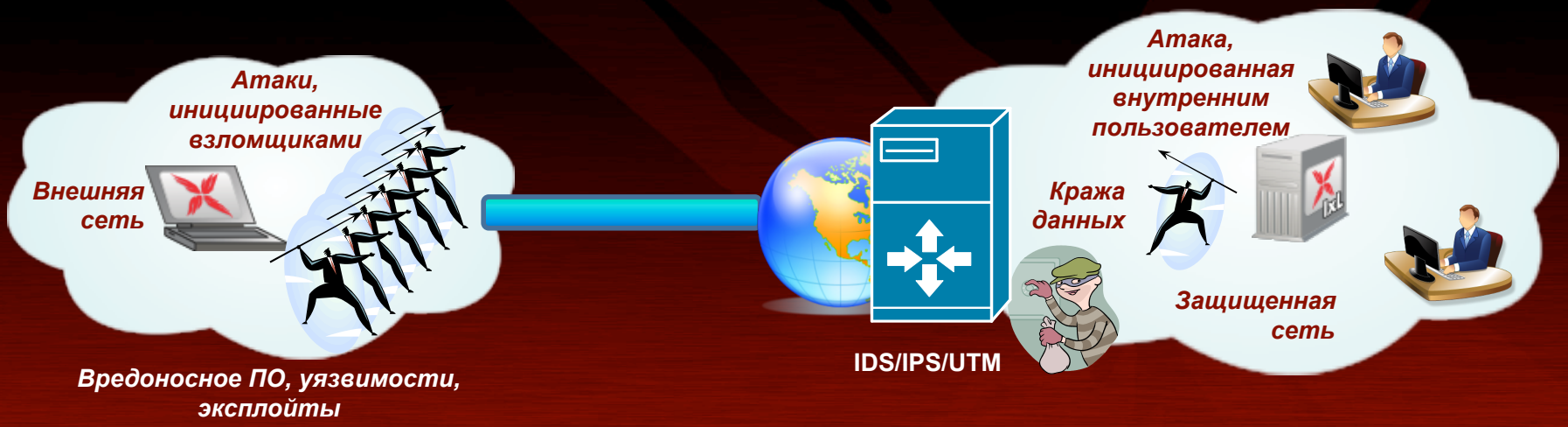
Определить как изменяется производительность тестируемого устройства при осуществлении атак через него.

Тестируемые устройства:

Устройства IDS/IPS или UTM, обнаруживающие и блокирующие атаки.

Метод тестирования:

Подключить тестируемое устройство к группе портов Ixia. Последовательно инициировать трафик атак без фонового трафика. Повторить это при наличии фонового трафика.



Тест №3: распространение вредоносного ПО через туннель IPsec

Цель:

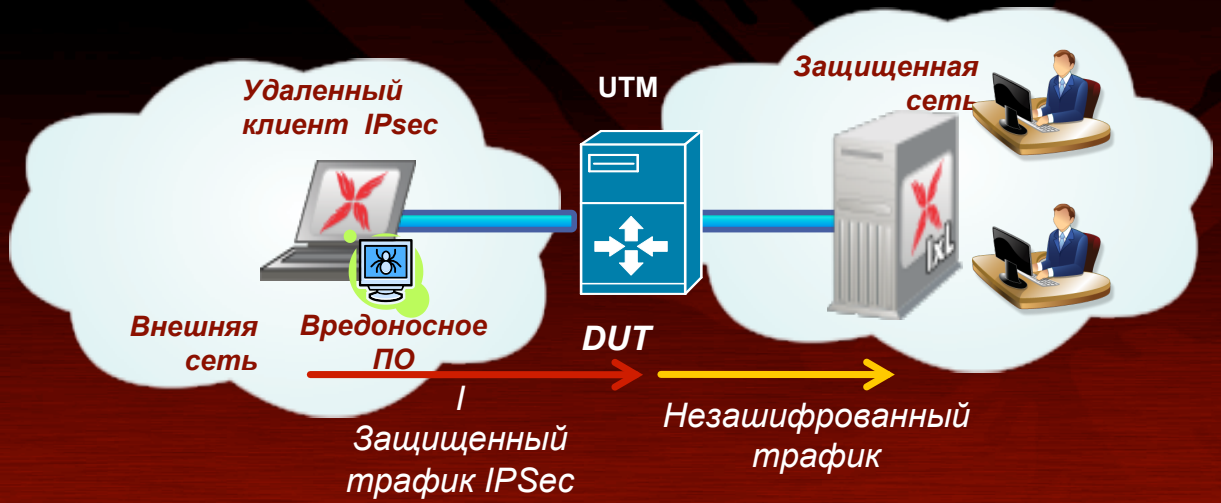
Протестировать эффективность работы защитного устройства и определить изменение его производительности при передаче вредоносных программ по туннелю IPsec от удаленных офисов или пользователей.

Тестируемые устройства:

Интегрированные защитные устройства (UTM, межсетевые экраны нового поколения).

Метод тестирования:

Подключить тестируемое устройство к группе портов Ixia. Сымитировать оконечные точки IPsec, передающие вредоносные программы по защищенному туннелю IPsec, который заканчивается на тестируемом устройстве.



Тест №4: атаки DoS/DDoS

Цель:

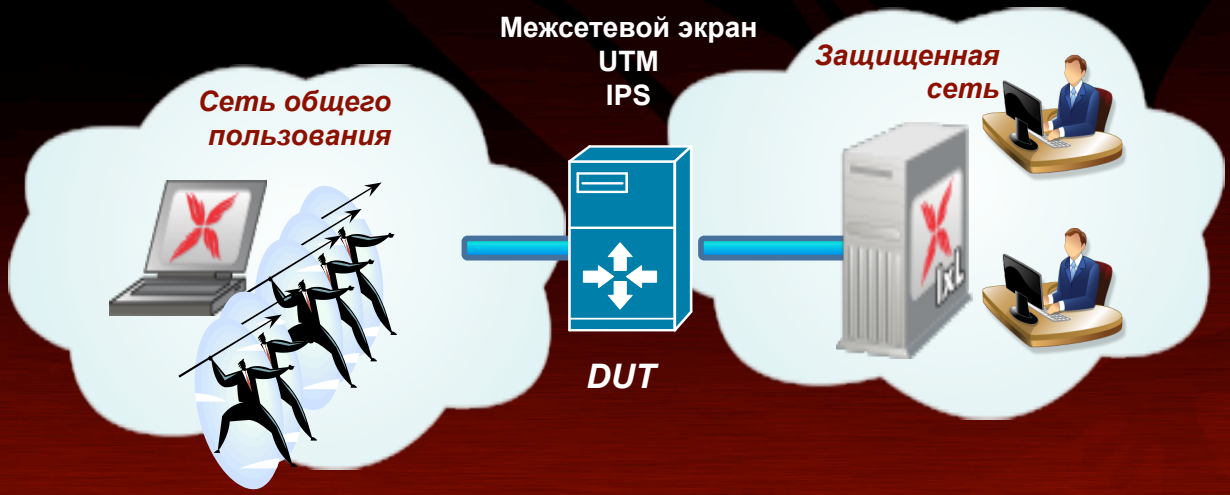
Проверить эффективность работы устройства защиты сети при имитации атак DoS/DDoS вперемешку с фоновым трафиком multiplay.

Тестируемые устройства:

Межсетевые экраны, UTM-устройства, системы IPS.

Метод тестирования:

Подключить тестируемое устройство к группе портов Ixia. Инициировать атаки DoS/DDoS и определить «предел прочности» устройства.



Спасибо!