s•terra®

Ваш ориентир в мире безопасности

Особенности измерения производительности систем обнаружения вторжений

www.s-terra.ru

Существующие наработки

s•terra®

- Опыт измерения производительности шлюзов безопасности (IPsec)
- Инструменты автоматического измерения производительности
- Знание основных факторов, влияющих на производительность IPsec

Производительность СОВ vs IPsec

Измерение производительности СОВ сложнее по сравнению с производительностью IPsec по ряду причин:

- Существенно большее количество факторов, влияющих на производительность СОВ
- Сложнее контроль корректности работы СОВ
- Вопросы составления эталонного образца трафика и получения зависимости количества ожидаемых обнаруженных инцидентов от скорости трафика
- «Срок жизни» результатов измерений

Известные стандарты и источники

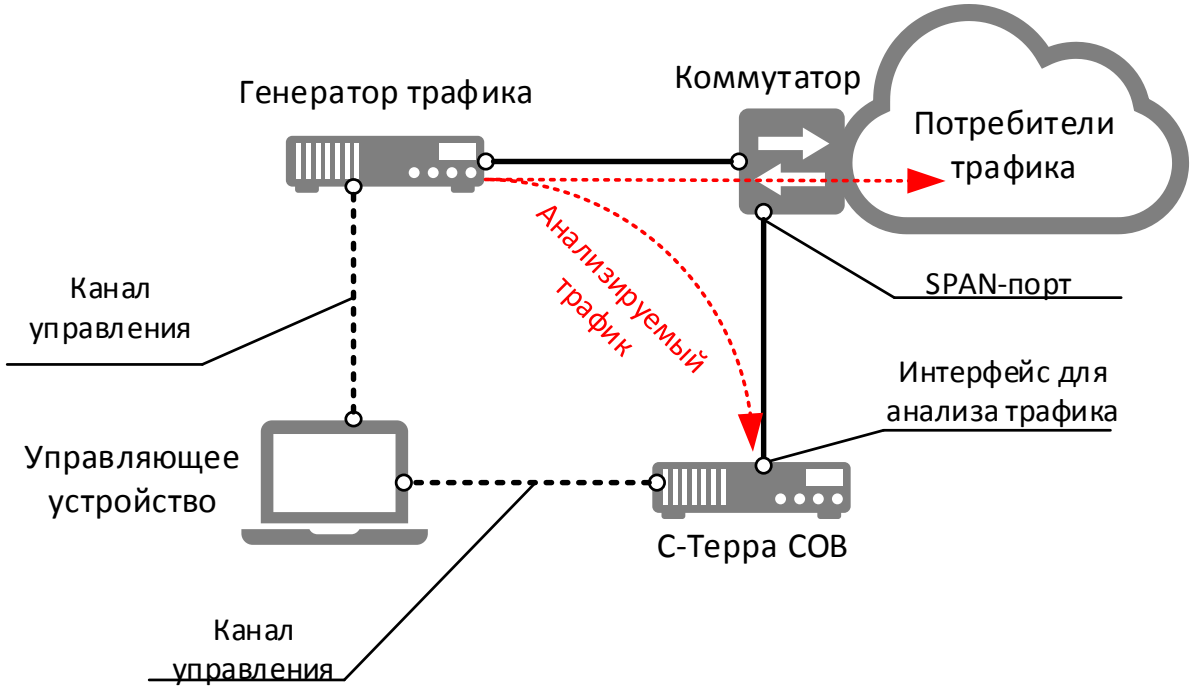
s•terra

- Уровень стандартизации процесса измерения производительности СОВ достаточно низкий (по сравнению с, например, процессом измерения производительности межсетевых экранов)
- Наиболее известный публичный, не зависящий от конкретного вендора документ:

NSS Labs. Test Methodology – Network Intrusion Prevention Systems v7.2 (https://www.nsslabs.com/linkservid/C2BADE48-5056-9046-935977F09AFC2546/)

- Помимо непосредственно производительности, документ описывает ряд других измеряемых и проверяемых параметров (эффективность защиты, стабильность, управляемость, совокупная стоимость владения)

Стенд измерения производительности



Предварительная подготовка к измерению

- На генераторе трафика подготавливается тестовый трафик. Используется запись трафика, содержащего в себе инциденты, которые должны быть идентифицированы, как компьютерные атаки. Для выбранной записи трафика и фиксированного набора правил известно точное количество таких инцидентов. Если количество инцидентов зависит от того, на какой скорости проигрывается трафик, то эта зависимость учитывается. Таким образом, для любой скорости проигрывания трафика мы знаем ожидаемое количество обнаруженных инцидентов.
- На устройстве С-Терра СОВ в дополнение к обычному набору правил добавляется вручную правило реагирующее на ping до определенного адреса.

Схема проведения измерения

- На генераторе трафика при помощи утилиты tcpreplay проигрывается подготовленная ранее запись трафика с заданной скоростью. Трафик может проигрываться несколько раз по кругу, с тем, чтобы при заданной скорости тест составил не менее 1 минуты.
- Одновременно запускается 1000 ping-пакетов с таким интервалом, чтобы посылка этих пакетов завершилась одновременно с завершением работы tcpreplay.
- Известно количество инцидентов в записанном трафике с учетом скорости, также известно, что каждый пинг-пакет должен быть зарегистрирован как инцидент. С учетом этого мы знаем ожидаемое количество зарегистрированных событий на С-Терра СОВ
- Если С-Терра СОВ удалось зарегистрировать эти инциденты, то данная скорость является допустимой для него и мы можем повторить процедуру измерения с более высокой скоростью. Если же часть инцидентов не была зарегистрирована, то скорость наоборот понижается.

Инструментарий

- python 3
- tcpreplay
- tcprewrite
- Набор записанных и/или сформированных pcap-файлов

Характеристики трафика (пример)

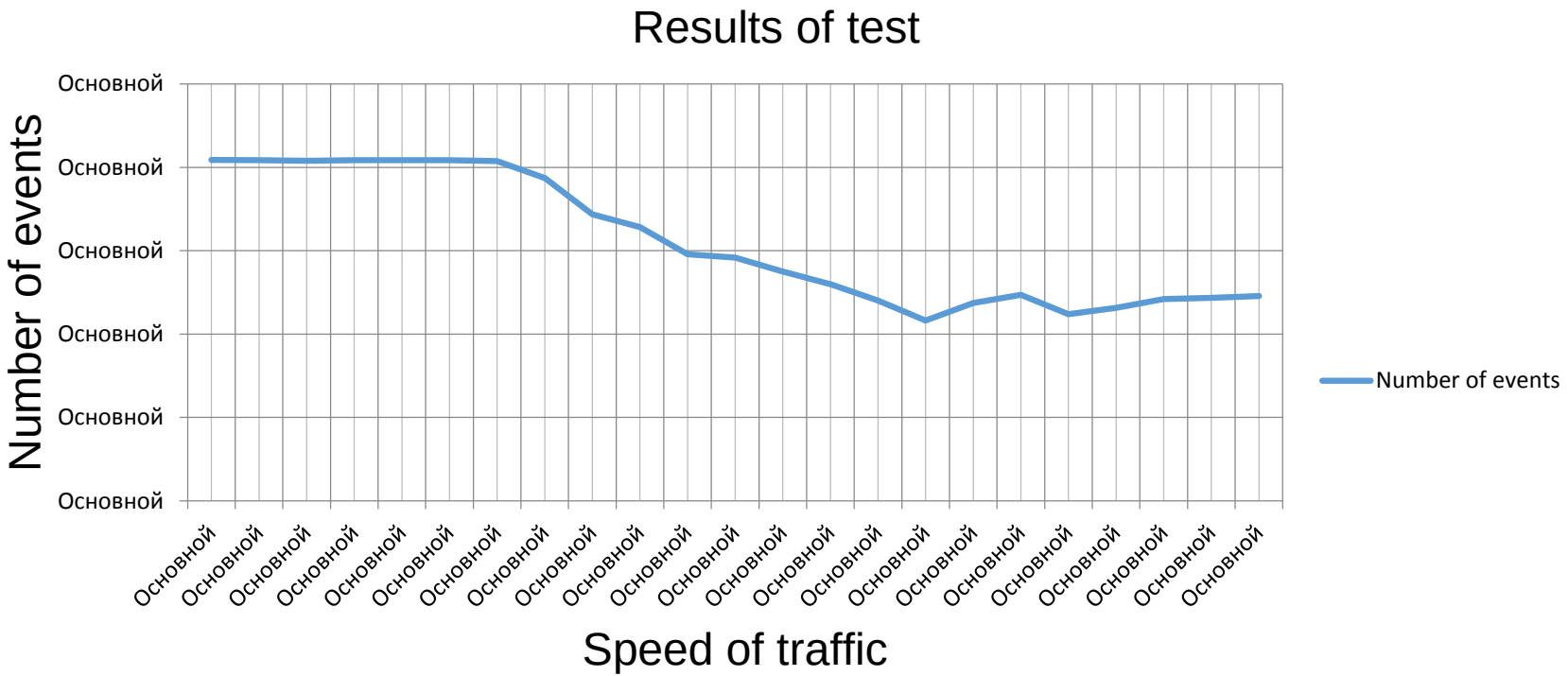
Display

Display filter: nor

Ignored packets: 0 (0

Traffic	Captured	Displayed
Bytes	935351586	935351586
Packets	1258366	1258366
Avg. packet size	743 bytes	
Avg. packets/sec	5048,788	
Avg. bytes/sec	3752797,103	
Avg. MBit/sec	30,022	
Between first and last packet	249,241 sec	

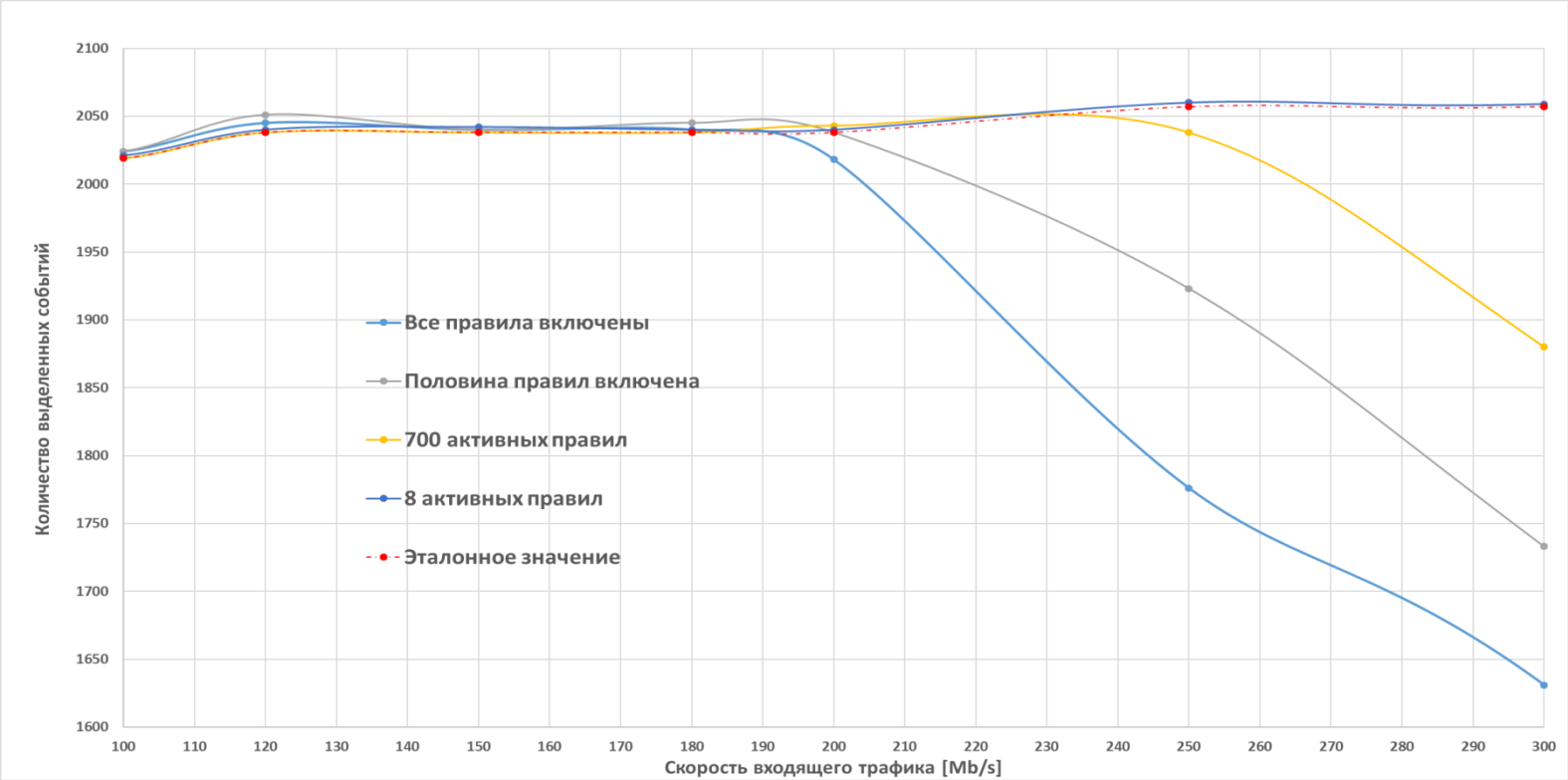
Типовой результат измерения



Существенно влияющие факторы

- Состав и количество сигнатур
- Характеристики трафика:
  - количество пакетов в секунду
  - средний размер пакетов
  - плотность инцидентов
  - состав инцидентов

Зависимость от количества сигнатур (правил)



Совместная работа COB и IPsec

s•terra

Производительность COB совместно с IPsec для платформ начального и среднего уровня

Процент потерянных пакетов при шифровании		скорость шифрования, Mbps			
		10	21	32	43
Скорость анализа трафика, Mbps	11	0.0%	0.0%	0.0%	3.0%
	22	0.0%	0.0%	2.0%	
	33	0.0%			
	45				

Процент потерянных пакетов при шифровании		скорость шифрования, Mbps			
		200	400	600	800
Скорость анализа трафика, Mbps	250	0.0%	0.00%	0.3%	15.0%
	450	0.0%	0.00%	2.0%	
	700	0.0%	0.05%	2.0%	17.0%
	900	0.0%	0.06%	2.8%	17.0%

Процент потерянных инцидентов при анализе		скорость шифрования, Mbps			
		10	21	32	43
Скорость анализа трафика, Mbps	11	0.0%	0.0%	0.0%	
	22	1.0%	0.0%	3.0%	
	33	25.0%	27.0%		
	45				

Процент потерянных инцидентов при анализе		скорость шифрования, Mbps			
		200	400	600	800
Скорость анализа трафика, Mbps	250	0.0%	0.0%	0.0%	0.0%
	450	0.0%	0.0%	0.0%	
	700	0.0%	0.0%	0.0%	40.0%
	900	0.0%	0.0%	0.0%	

Москва, г. Зеленоград, Георгиевский пр-кт, дом 5

+7 (499) 940 9001

sales@s-terra.ru, www.s-terra.ru

s•terra®