SLA в услуге Anti-DDoS

Мирошниченко И.В.

Руководитель группы управления продуктами РТКОММ

Апрель 2010, Москва

РТКОММ
группа компаний РОСТЕЛЕКОМ

Содержание

- Текущая ситуация с SLA
- Основные параметры услуги
- Формализация DDoS-атаки - возможно ли такое?
- От уровня данных к уровню сервиса

РТКОММ
группа компаний РОСТЕЛЕКОМ

SLA?

У вас обнаружили $ %$#@?

Вылечим на 80%!!!

РТКОММ
группа компаний РОСТЕЛЕКОМ

SLA?

Наши бронежилеты защитят вас от выстрела из Webley&Scott 1905 г.в. на 99,5%!!!

РТКОММ
группа компаний РОСТЕЛЕКОМ

SLA?

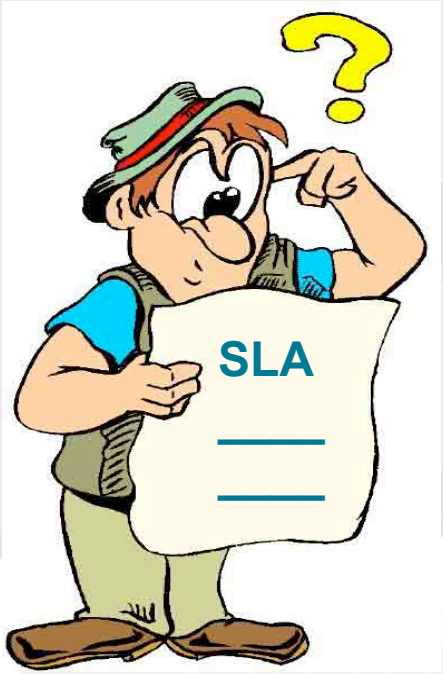
№	Тип Атаки	Средний % очистки	Средний % прохождения легитимных
1.	нелегитимный трафик на невостребованный протокол и/ или порт (пример — UDP Flood, ICMP Flood)	98%	98%
2.	инициация соединения по протоколу TCP (SYN-Flood) со случайной подменой IP-адреса отправителя данных (IP-Spoof)	98%	98%
3.	установка полноценного TCP-соединения и с его дальнейшим сбрасыванием без обмена данными внутри сокета (TCP Connect Flood)	98%	98%
4.	отказ в обслуживании сервиса/ресурса атакой по протоколу HTTP/1.0 или HTTP/1.1 путем отправки данных: 1.вне спецификации протокола; 2. по спецификации протокола без дальнейшего следования инструкциям перенаправления (HTTP Redirect, JavaScript Redirect); 3. по спецификации протокола с дальнейшим следованием инструкций перенаправления против защиты на уровне теста Тьюринга (captcha).	98%	98%
5.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае наличия криптографического сертификата на фильтрующих ресурсах	98%	98%
6.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае отсутствия сертификата на фильтрующих ресурсах	80%	80%
7.	фильтрация трафика в условиях наличие большого количества легитимных пользователей ресурса с генерацией трафика разных характеристик	80%	80%
8.	атака по протоколу DNS с генерацией легитимных запросов	80%	80%
9.	Иные типы атак	75%	

Этого достаточно?

РТКОММ
группа компаний РОСТЕЛЕКОМ

Основные параметры SLA

- Время реакции на DDoS-атаку
- Доступность услуги отражения DDoS
- Процент пропущенного трафика DDoS
- Процент пропущенного трафика не-DDoS
- Список отслеживаемых протоколов на наличие DDoS
- ……

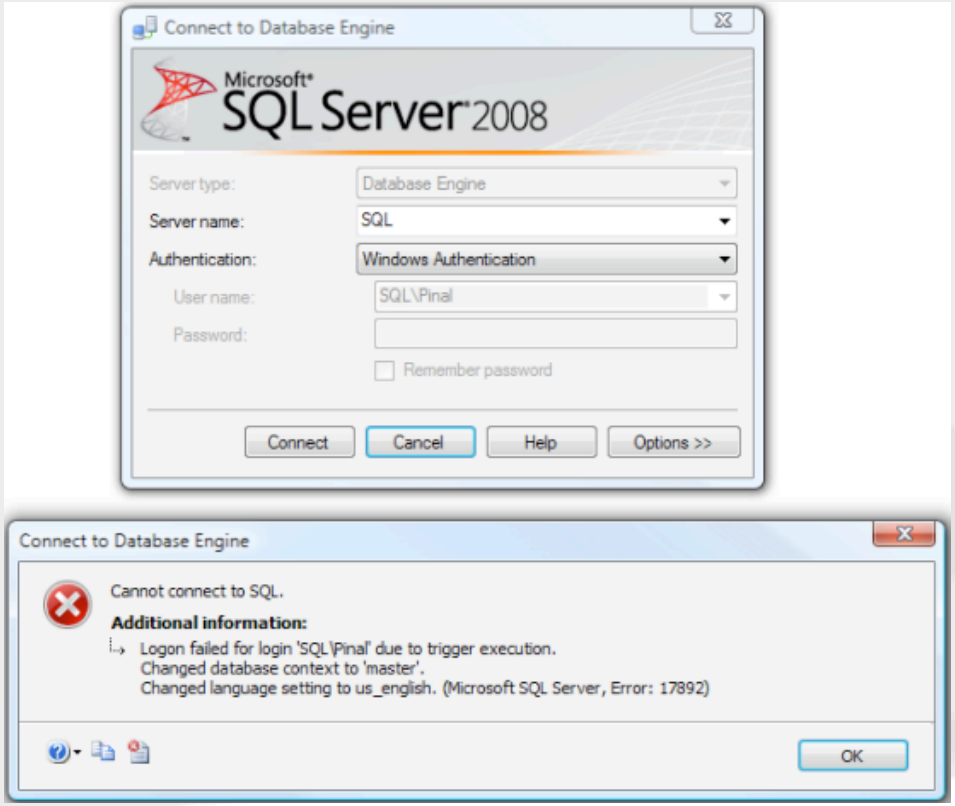


Клиент: Есть ли формальное всеобъемлющее вневременное определение DDoS?

РТКОММ
группа компаний РОСТЕЛЕКОМ

Основные параметры SLA

- .....
- Время восстановления сервиса Интернет



Клиент: А когда пользователи смогут нормально работать с приложениями?

РТКОММ
группа компаний РОСТЕЛЕКОМ

Давайте обсудим!

РТКОММ
группа компаний РОСТЕЛЕКОМ