Анализ актуальных угроз внешних атак на финансовые структуры

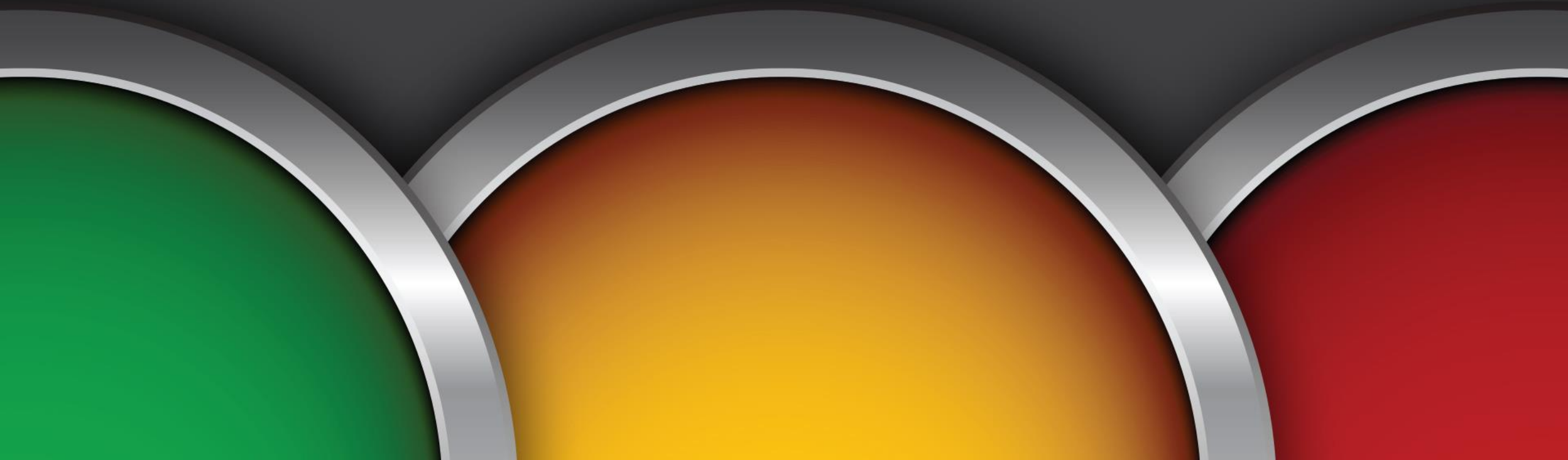
Михаил Суконник

Руководитель группы СНГ и Прибалтики

Radware Ltd

radware
Every second counts

Изменения в атаках в конце 2015 года



Radware AMS

Radware Attack Mitigation System (AMS) защищает

- 7 из 14 крупнейших мировых бирж
- 12 из 22 крупнейших мировых банков
- Крупнейшие страховые компании
- 6 из 20 крупнейших ретэйлеров и их платежные системы
- Десятки банковских и финансовых организаций в РФ

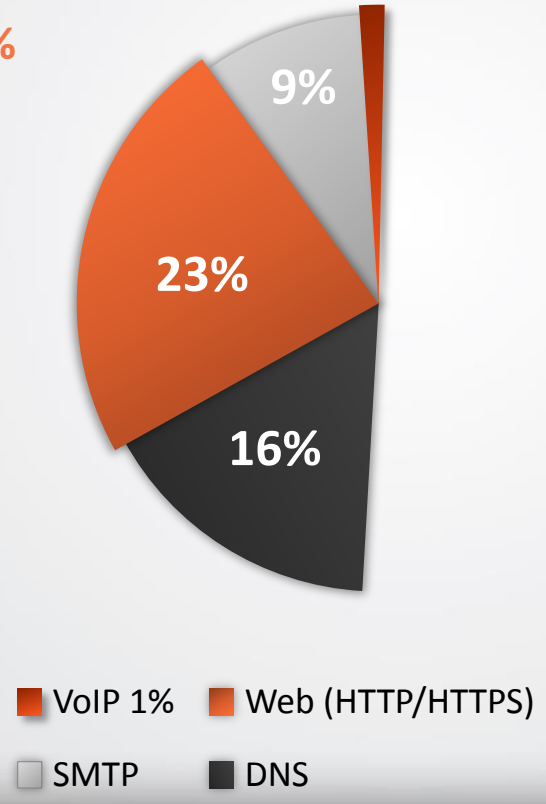
Основные причины атак

- Рост финансово мотивированных атак (2015 год)
- Политически мотивированные атаки (рост с конца 2014 года)

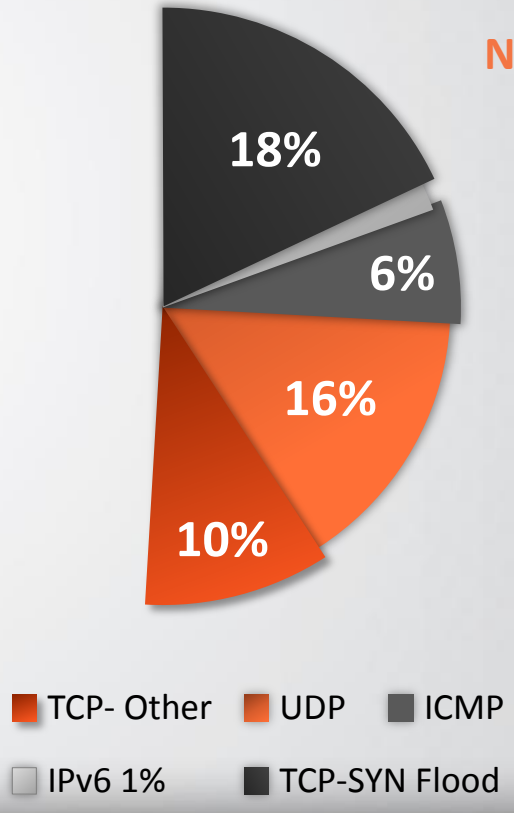
Многовекторность

- Одновременное использование 4-10 векторов атаки
- Одновременные DDoS атаки на 3-7 уровне и атаки на уровне WEB (QWASP 10)

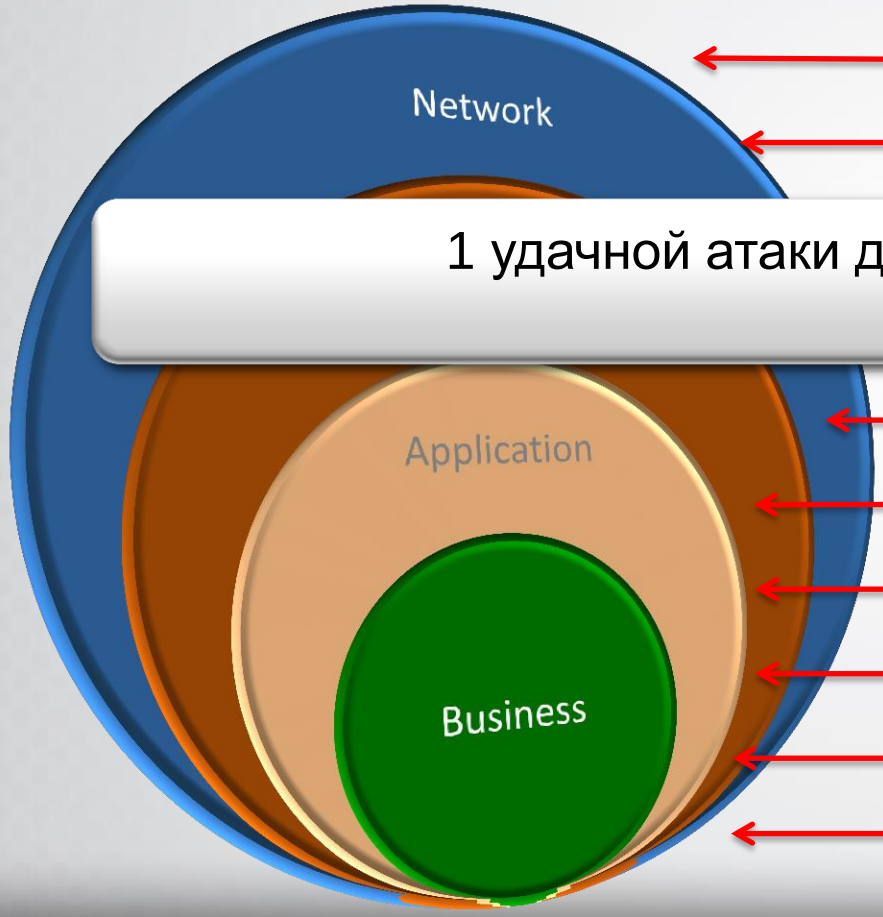
Application 49%



Network 51%



Многовекторность



Volumetric network flood attacks

Network scan

Intrusion

Port scan

1 удачной атаки достаточно чтобы заблокировать сервис

“Low & Slow” attacks

Application Flood attacks

Application vulnerability, malware

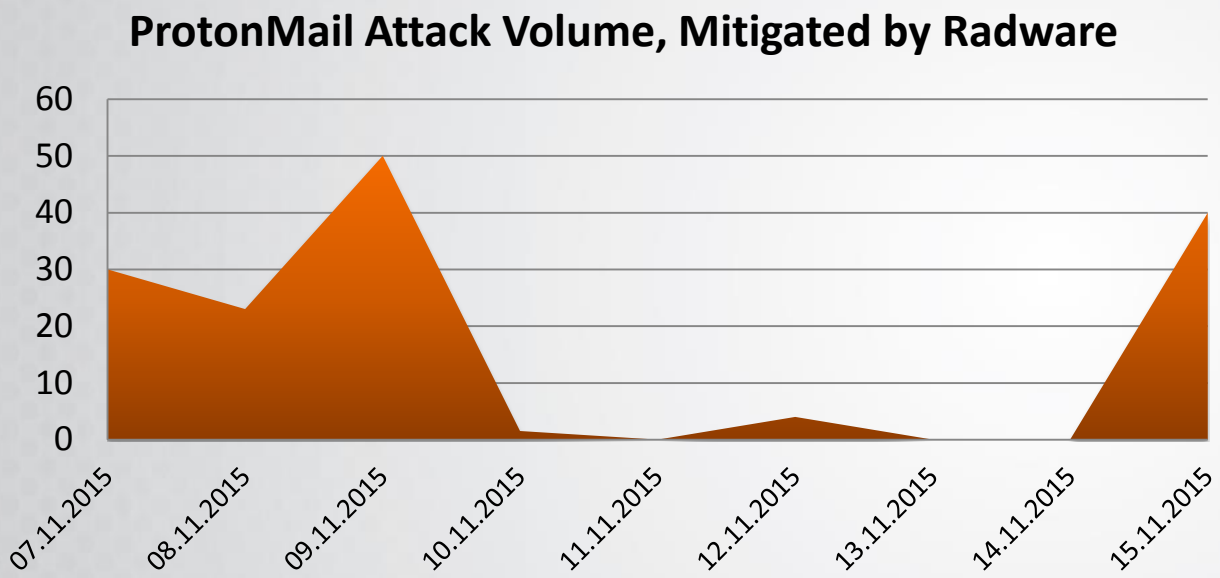
SSL based attacks

Web attacks: XSS, Brute force

Web attacks: SQL Injection

ProtonMail

Persistent Denial of Service Attacks



Network	Application
UDP Flood	DNS Reflection
TCP RST Flood	NTP Reflection
TCP-SYN	SSDP
TCP Out-of-State	HTTP/S SYN Flood
SYN-ACK	
ICMP	

Help Net Security @helpnetsecurity · Nov 10
ProtonMail restores services after epic DDoS attacks - bit.ly/1WKzc6N - @**ProtonMail** @**radware** @CarlHerberger

ProtonMail @ProtonMail · Nov 10
We want to give our thanks to @ip_max and @**radware**, without their support, we would not be online today. protonmail.com/blog/protonmai...

Угроза от небольших атак

- По данным Центра Касперского успешная атака на 5 крупных банков (конец 2014) имела мощность **20 Мбс** (!)
- Атака Anonymous на финансовые структуры 8-9.02.16 использовала LOIC, HOIC, XOIC – медленные атаки
- Атаки под SSL

Автоматизация атак

- Изменение векторов атак в каждые несколько минут !

Автоматизация атак

Attack Name	Start Time	DOSS-NTP-reflected-monlist	01/31/2016 00:33:41	network flood IPv4 UDP	01/31/2016 00:23:10
network flood IPv4 UDP	01/31/2016 00:25:16	DOSS-NTP-reflected-monlist	01/31/2016 00:33:50	DOSS-tcp-zero-seq	01/31/2016 00:42:15
network flood IPv4 ICMP	01/31/2016 00:25:21	DOSS-NTP-reflected-monlist	01/31/2016 00:33:55	network flood IPv4 ICMP	01/31/2016 00:41:40
network flood IPv4 ICMP	01/31/2016 00:27:51	DOSS-NTP-reflected-monlist	01/31/2016 00:34:01	network flood IPv4 UDP	01/31/2016 00:42:30
DOSS-NTP-reflected-monlist	01/31/2016 00:32:31	DOSS-SSDP-reflected	01/31/2016 00:33:25	network flood IPv4 ICMP	01/31/2016 00:45:26
DOSS-NTP-reflected-monlist	01/31/2016 00:32:35	DOSS-SSDP-reflected	01/31/2016 00:33:26	network flood IPv4 UDP	01/31/2016 00:42:41
DOSS-NTP-reflected-monlist	01/31/2016 00:32:46	DOSS-NTP-reflected-monlist	01/31/2016 00:35:00	DOSS-DNS-Ref-L4-Above-3000	01/31/2016 01:43:33
DOSS-NTP-reflected-monlist	01/31/2016 00:33:16	DOSS-SSDP-reflected	01/31/2016 00:34:55	DOSS-DNS-Ref-L4-Above-3000	01/31/2016 01:43:36
DOSS-DNS-Ref-L4-Above-3000	01/31/2016 00:23:05	DOSS-SSDP-reflected	01/31/2016 00:36:06	network flood IPv4 UDP	01/31/2016 01:43:36
DOSS-NTP-reflected-monlist	01/31/2016 00:33:36	network flood IPv4 ICMP	01/31/2016 00:23:25	network flood IPv4 ICMP	01/31/2016 01:43:33
DOSS-DNS-Ref-L4-Above-3000	01/31/2016 00:22:51	DOSS-SSDP-reflected	01/31/2016 00:36:05	network flood IPv4 ICMP	01/31/2016 01:43:36
DOSS-NTP-reflected-monlist	01/31/2016 00:33:40	network flood IPv4 ICMP	01/31/2016 00:30:31		
		network flood IPv4 UDP	01/31/2016 00:30:31		

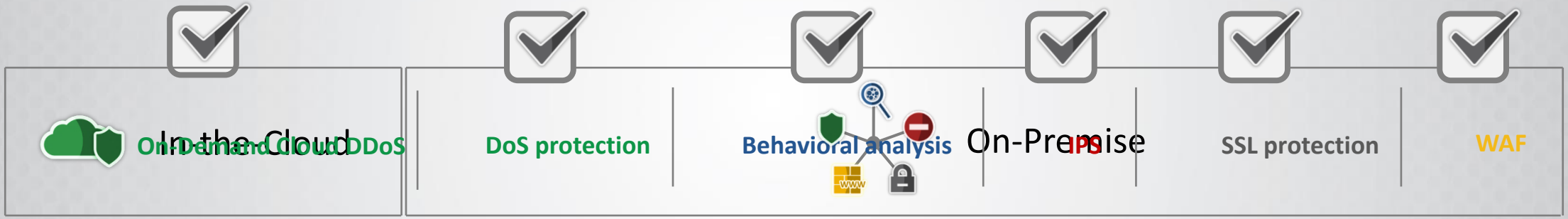
Признак атакующего

- IP адрес все чаще невозможно использовать (или – его недостаточно) для блокировки атаки

Выводы- минимальные требования к отражению

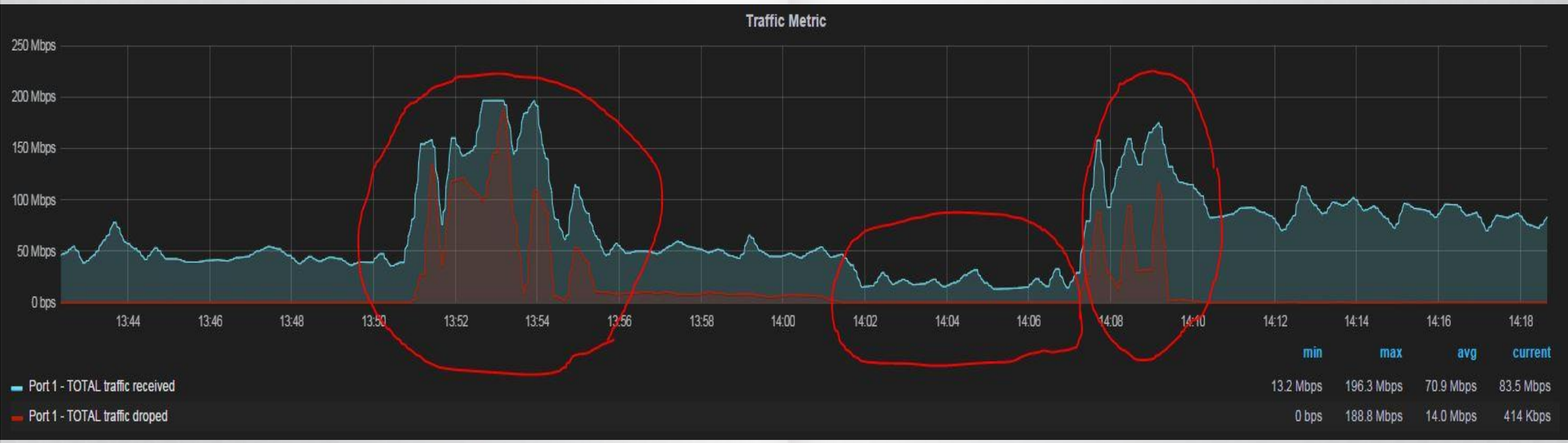
- Система должна обеспечивать работу легитимных пользователей под атакой !
- Система должна отражать все атаки !
- Система должна блокировать атаки на приложения без ущерба легитимным клиентам, включая атаки под SSL
- Система должна работать автоматически – без ручных настроек под атакой
- Полное решение может включать CPE и услугу для защиты от мощных сетевых флудов

AMS – многоуровневая защита



Задача – автоматически обеспечить доступность легитимных клиентов под атакой на основе Поведенческого анализа легитимных клиентов на различных уровнях

Реальная атака на фин. структуру – September – CPE – NTP reflection + HTTP



radware

Every second counts