10 YEARS JETSECURITY CONFERENCE 2019

МУКИ ВЫБОРА ИЛИ КАК ПОСТРОИТЬ БЕЗОПАСНУЮ ЗАЩИТУ WEB ТРАФИКА

Денис Шуров

Начальник отдела внедрения, развития и технической поддержки СЗИ
Тел: +7 /812/ 329 5000*6499 email: denis.a.shurov@bspb.ru

БАНК САНКТ-ПЕТЕРБУРГ

ЧТО ИМЕЕМ – ЧЕМ ЗАЩИЩАЕМ

БСПБ

УГРОЗЫ И УЯЗВИМОСТИ

- Сетевые атаки на ОС пользователей
- Сетевые атаки на браузер
- Внедрение ВПО из сети Интернет
- Несанкционированный доступ к внешним ресурса

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ

- Next-Generation Firewall (NGFW)
- Secure Web gateway (SWG)

«A Secure Web gateway (SWG) is a solution that filters unwanted and malicious software (malware) from user-initiated Web/Internet traffic, and enforces corporate Internet policy compliance. SWGs must, at a minimum, include URL filtering, malicious code detection and filtering, and application controls for popular Web-based applications. Native or integrated content-aware data loss prevention (DLP) is also increasingly included. SWGs have traditionally been appliances and software. However, the cloud-based SWG delivery model is growing rapidly.»

Gartner

«The firewall market has evolved from simple stateful firewalls to NGFWs, incorporating full-stack inspection to support intrusion prevention, application-level inspection and granular policy control. Such NGFWs will eventually subsume mainstream deployments of stand-alone network intrusion prevention system (IPS) appliance technology at the enterprise edge.»

Gartner

10 YEARS JETSECURITY CONFERENCE 2019

ДВА РЕШЕНИЯ, ДВА ПУТИ ИЛИ…?

БСПБ

NGFW

SWG

10 YEARS JETSECURITY CONFERENCE 2019

СЛОЖНЫЙ ВОПРОС, А ОДНОЗНАЧЕН ЛИ ОТВЕТ?

БСПБ

Функции	NGWF	SGW
AV – защита от «вредоносов»	√	√
AppFiltering – определение и фильтрация приложений	√	√
Anti-bot – блокирование ботнет	√	√
DLP – выявление утечек информации	√	√

Имеется / Требуется		Дополняем / Внедряем
Firewall	+	SWG
Proxy	+	NGFW
Удаленные подразделений с собственными каналами	→	NGFW
Обеспечить только функции защиты и фильтрации	→	SWG

10 YEARS JETSECURITY CONFERENCE 2019

МУКИ ВЫБОРА И МНОГОУРОВНЕВАЯ ЗАЩИТА

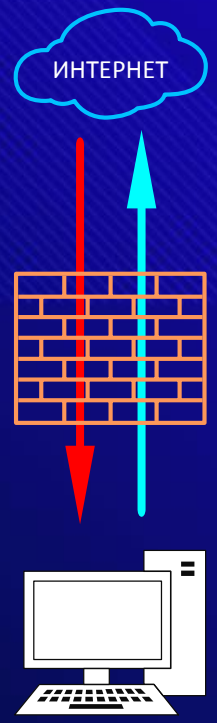
БСПБ

Bluecoat ProxySG целенаправленно разработан для повышения уровня безопасности:

- NGWF только современный межсетевой экран с некоторыми расширенными функциями, что менее безопасно, чем в архитектуре с ProxySG

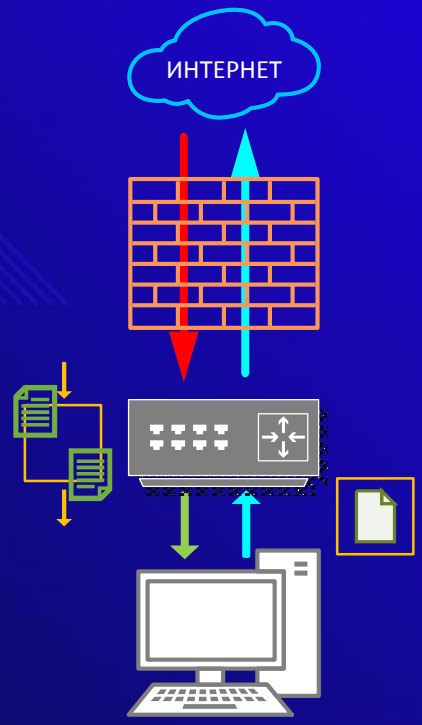
- NGWF использует потоковые методики обнаружения, исследую трафик по мере его прохождения, в то время как, ProxySG анализирует объект целиком (дожидается сборки пакета)

NGFW



- No termination
- Stream scanning only

NGFW+ WebProxy



- Session termination
- Policy enforcement
- Web proxy

10 YEARS JETSECURITY CONFERENCE 2019

КОНТРОЛЬ И АНАЛИТИКА

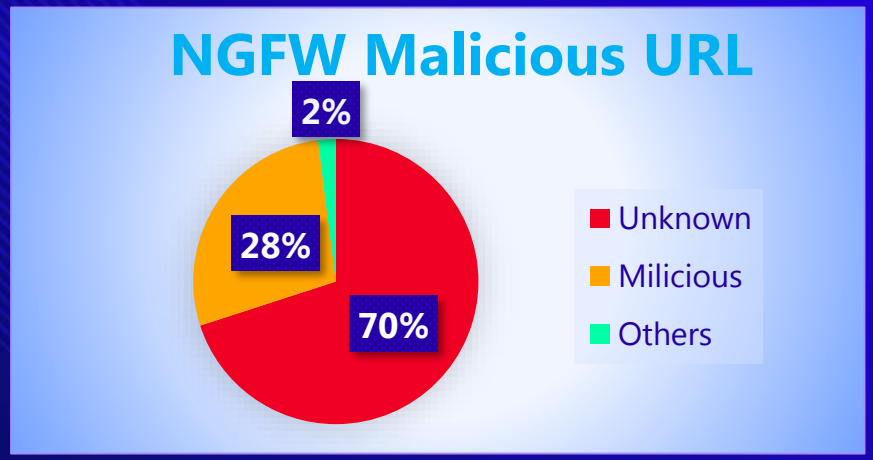
БСПБ

Облачные приложения, необходимость контроля и управления:

- ProxySG позволяет получать информацию и средства управления облачными приложениями
- Возможность применения ручной или рейтинговой системы контроля и ограничения использования приложения через ProxySG

Внешняя аналитика и разведка (GIN) :

- Точное классифицирование сайтов
- Оперативное обновление классификатора
- Whitelisting

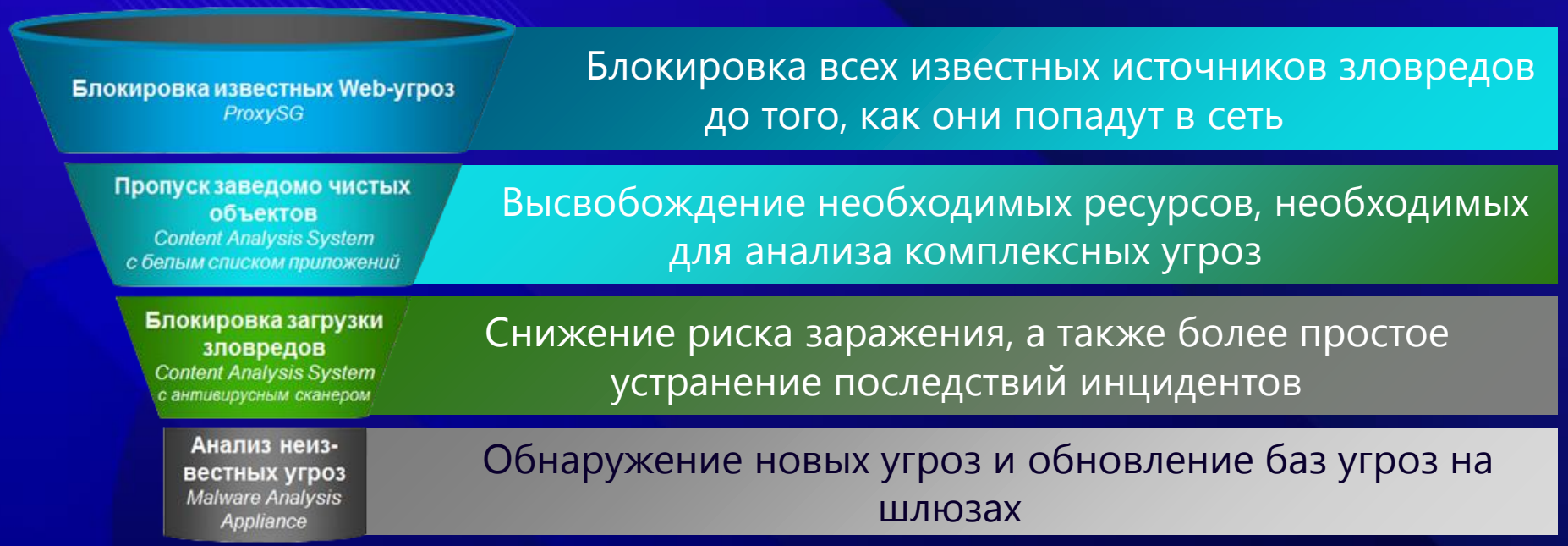


10 YEARS JETSECURITY CONFERENCE 2019

О НЕ ПРОСТОМ ВЫБОРЕ И НЕ ТОЛЬКО

БСПБ

- Заявленная общая производительность отличается от реальной
- Кэширование и оптимизация – преимущество и ускорение
- Гибкие настрой политик (VPM или CPL) – отличительная черта ProxySG
- Возможность гибкой и открытой интеграции с другими решения по безопасности
- «Правильная аутентификация»



10 YEARS JETSECURITY CONFERENCE 2019

ЗАКЛЮЧЕНИЕ

БСПБ

- Стандартный продвинутый подход для борьбы с киберугрозами – многоуровневая защита вашей сети, где, наряду с антивирусами на отдельных компьютерах, во всех точках входа в сеть извне установлены специальные веб-шлюзы (SGW). Преимущество наличия отдельного защищённого веб-шлюза заключается в том, что он, как правило, позволяет нейтрализовать инсайдерскую халатность или злой умысел.

- Остановить вал зловредства в настоящее время практически невозможно – если только не отключить интернет или запретить компьютеры, но гильотина как средство от головной боли не кажется оптимальным лекарством.

- Аксиома индустрии кибербезопасности в том, что совершенно необязательно быть на 100% защищённым, чтобы избежать 99,9% вирусов и попыток взлома. Не нужно делать систему полностью защищённой от любых попыток взлома. Защита просто должна быть надёжнее, чем у соседа, чтобы киберзлодеи ограбили его, а не вас.

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Денис Шуров

Начальник отдела внедрения, развития и технической поддержки СЗИ
Тел: +7 /812/ 329 5000*6499 email: denis.a.shurov@bspb.ru

БАНК САНКТ-ПЕТЕРБУРГ