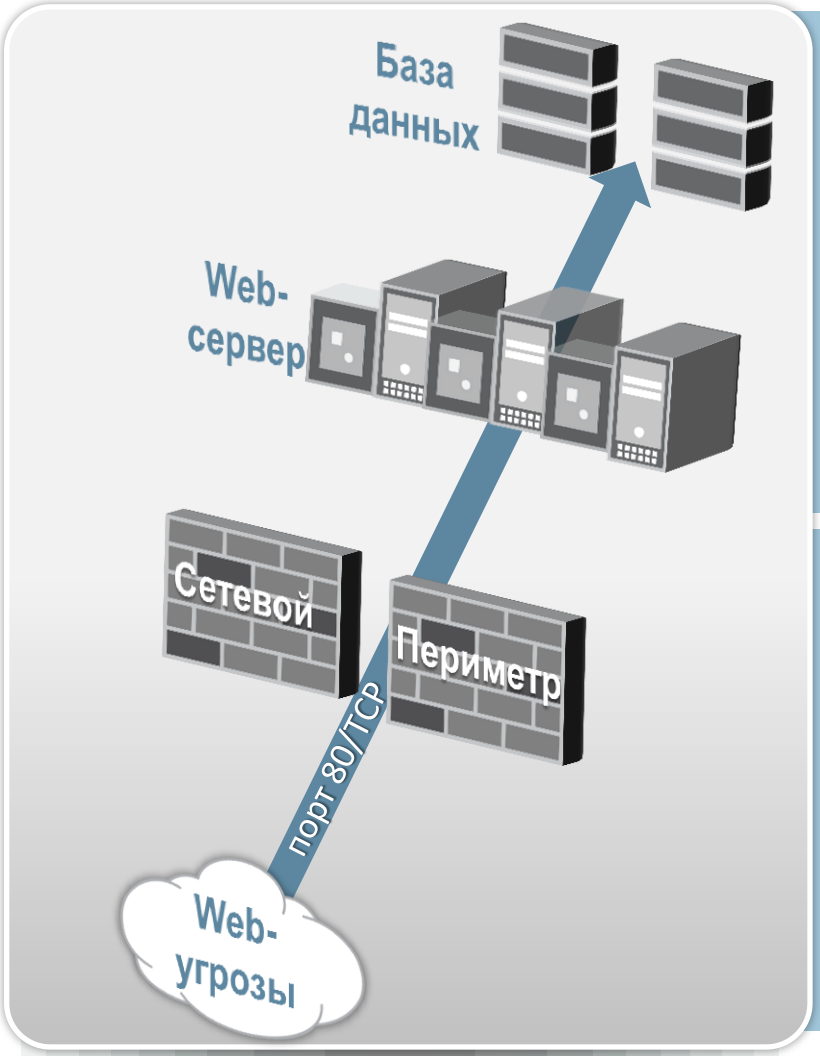
MYKONOS

ЛУЧШИЙ СПОСОБ ЗАЩИТИТЬ ВАШ WEB-САЙТ И WEB-ПРИЛОЖЕНИЕ ОТ АТАК

Павел Живов
Системный инженер
pzhivov@juniper.net
13 ноября 2012 г.

УГРОЗЫ WEB-ПРИЛОЖЕНИЙ

НАСТОРАЖИВАЮЩАЯ СТАТИСТИКА



70%

всех атак совершается на уровень Web-приложений

Gartner

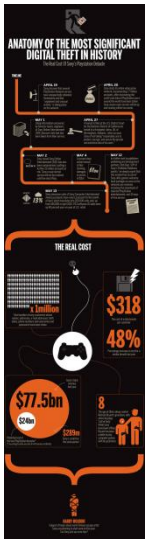
73%

подверглись атакам в течение последних двух лет через уязвимости web-приложений

Ponemon Institute

УЯЗВИМОСТИ СТОЯТ ДОРОГО

ИНСТИТУТ PONEMON | ОДНА УКРАДЕННАЯ ЗАПИСЬ СТОИЛА В СРЕДНЕМ $318



Sony
Украденных записей
77 млн.

Кража информации

Sony
Судебные издержки
$1-2 млрд.

Ухудшение репутации

Снижение доходов

Прямые издержки Sony
$171 млн.
- 23 дня простоя сети
- Потеря заказчиков

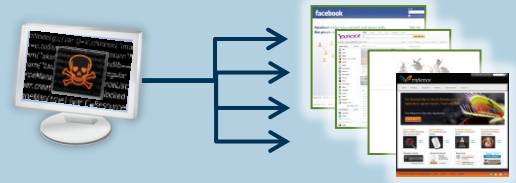
УГРОЗЫ, ИСХОДЯЩИЕ ОТ ХАКЕРОВ

Скрипты & Эксплоиты

Общие скрипты и инструменты хакеров

IP-сканирование

Поиск определенных уязвимостей при помощи скриптов на многих сайтах

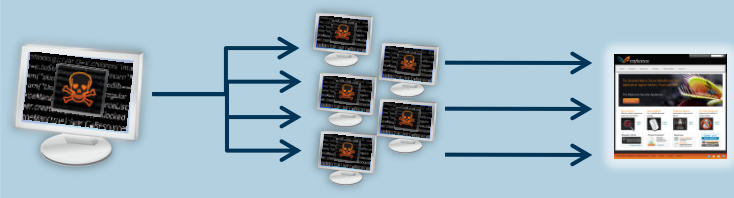


Целевое сканирование

Поиск уязвимостей определенного сайта

Ботнеты

Скрипты выполняются зараженными машинами и осуществляют атаку



Высококвалифицированные хакеры

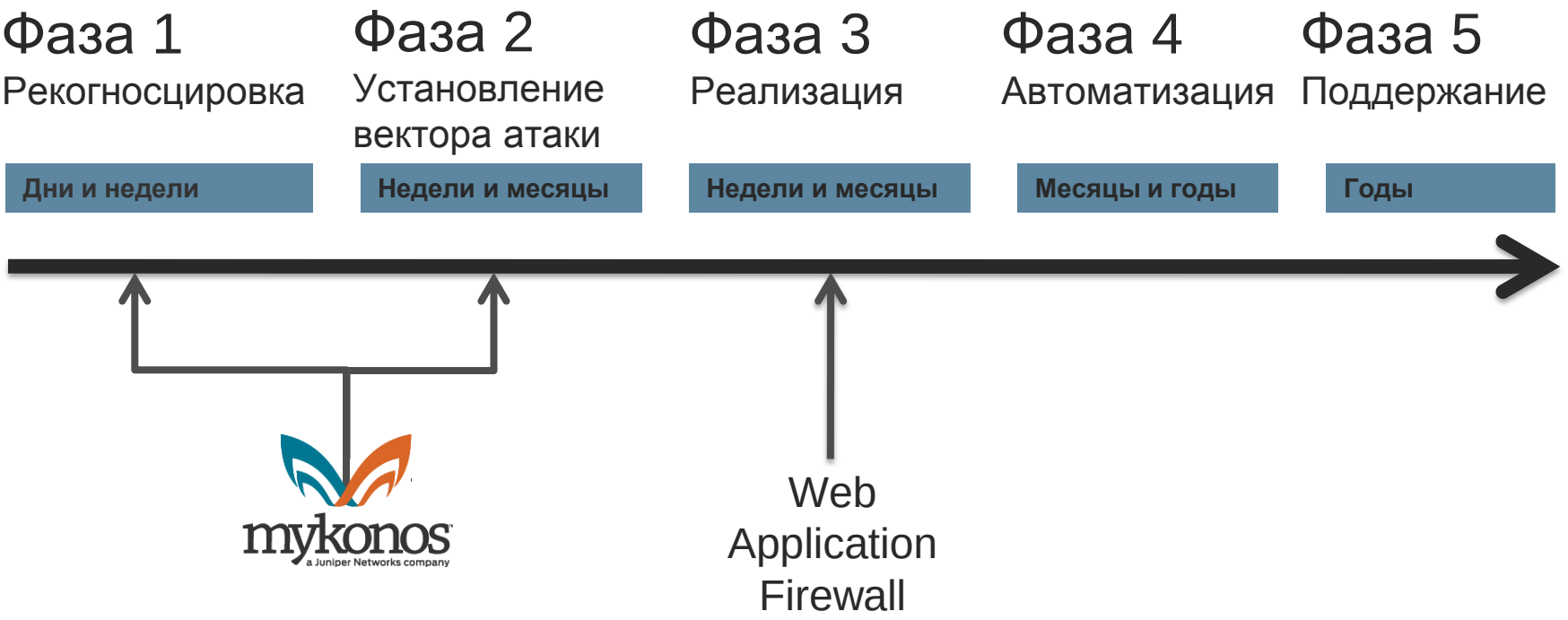
Сложные, целенаправленные атаки (APT).
Неторопливо и аккуратно, чтобы обойти защиту.

ОБЩИЕ ДАННЫЕ О MYKONOS WEB SECURITY

ПРОБЛЕМЫ ПРИ ИСПОЛЬЗОВАНИИ WEB APPLICATION FIREWALL

- Необходимы глубоки знания о защищаемых приложениях (и WAF, и администратору)
- При изменении приложения (например, обновление) требуется цикл настройки WAF так, чтобы не нарушить работу приложения
- Часто сложно найти глубокую техническую информацию по приложению для его защиты
- Многие приложения поставляются «из коробки» и трудно отслеживать наличие в них уязвимостей и их устранение
- Уязвимость к атакам «нулевого» дня
- Генерация большого количества ложных тревог

ФАЗЫ ВЕБ-АТАКИ



ПРЕИМУЩЕСТВА MYKONOS

- Ухудшает «экономику» атаки, делая ее очень затратной для хакера по времени и усилиям

- В отличие от WAF защищает от атак «нулевого дня»

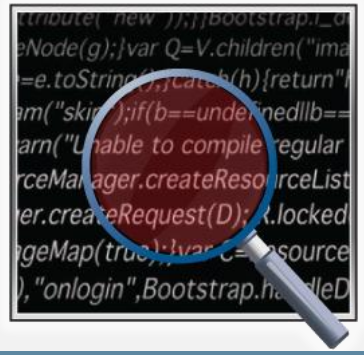
- В отличие от WAF практически не генерирует ложных тревог

- Обнаруживает атаку еще на этапе рекогносцировки и блокирует злоумышленника

- Минимальная настройка – работает «из коробки»

- Инновационная технология Intrusion Deception – нет аналогов на рынке

ПРЕИМУЩЕСТВА MYKONOS
БЕЗОПАСНОСТЬ НА ОСНОВЕ ОБМАНА ЗЛОУМЫШЛЕННИКА



Обнаружение

“Ловушки” обнаруживают угрозы без ложных срабатываний

Отслеживание

Отслеживается IP, параметры браузера, ОС и скриптов

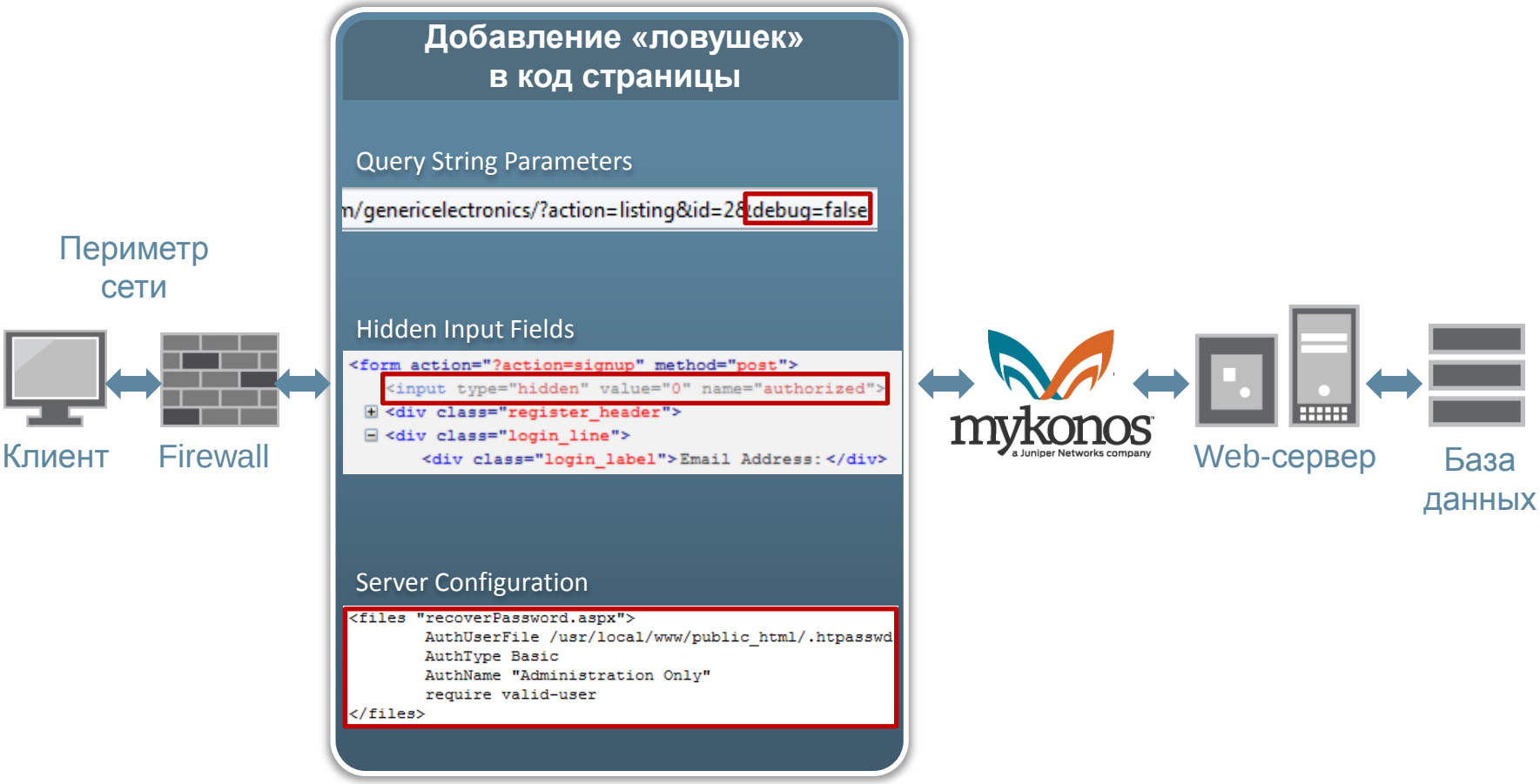
Профилирование

Понимание возможностей и намерений атакующего

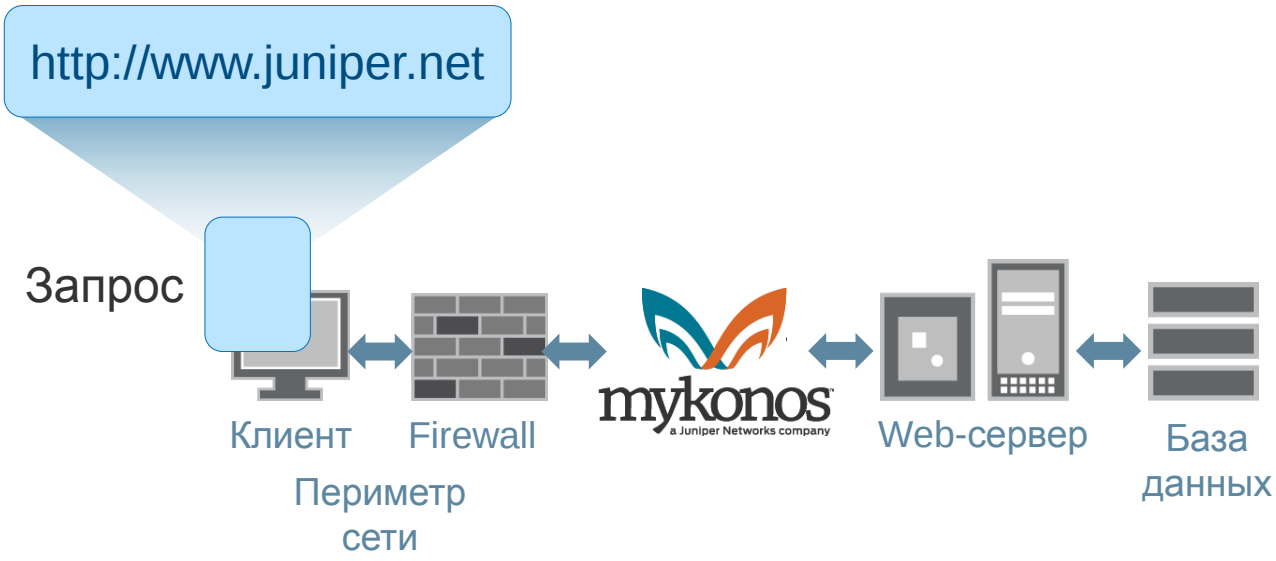
Реагирование

Адаптивная реакция, включающая блокировку предупреждение и обман

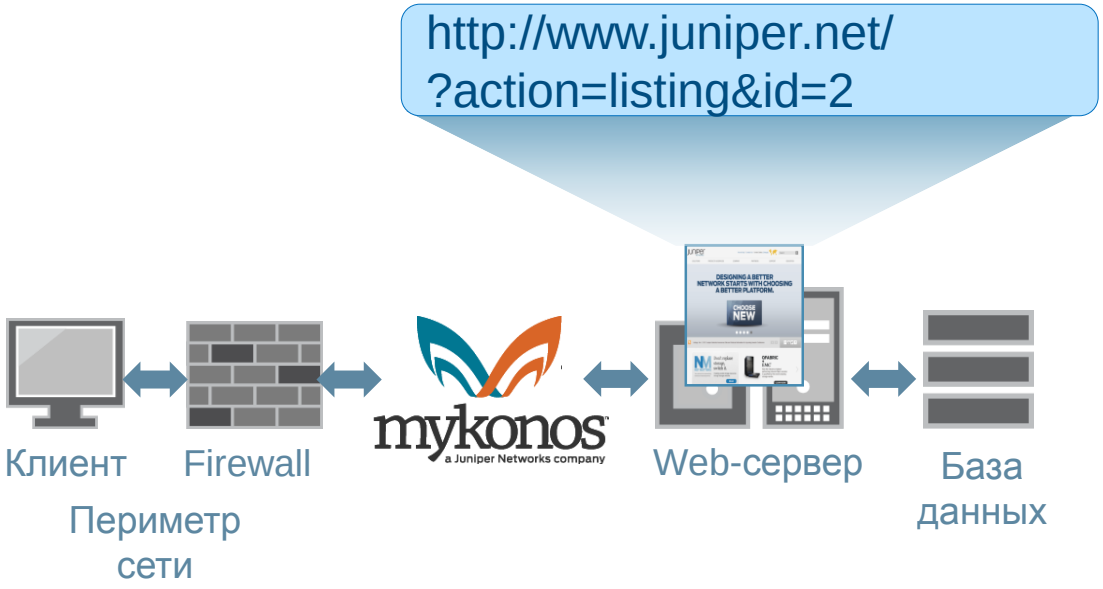
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Добавление ловушек в код страницы



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Добавление ловушек в код страницы

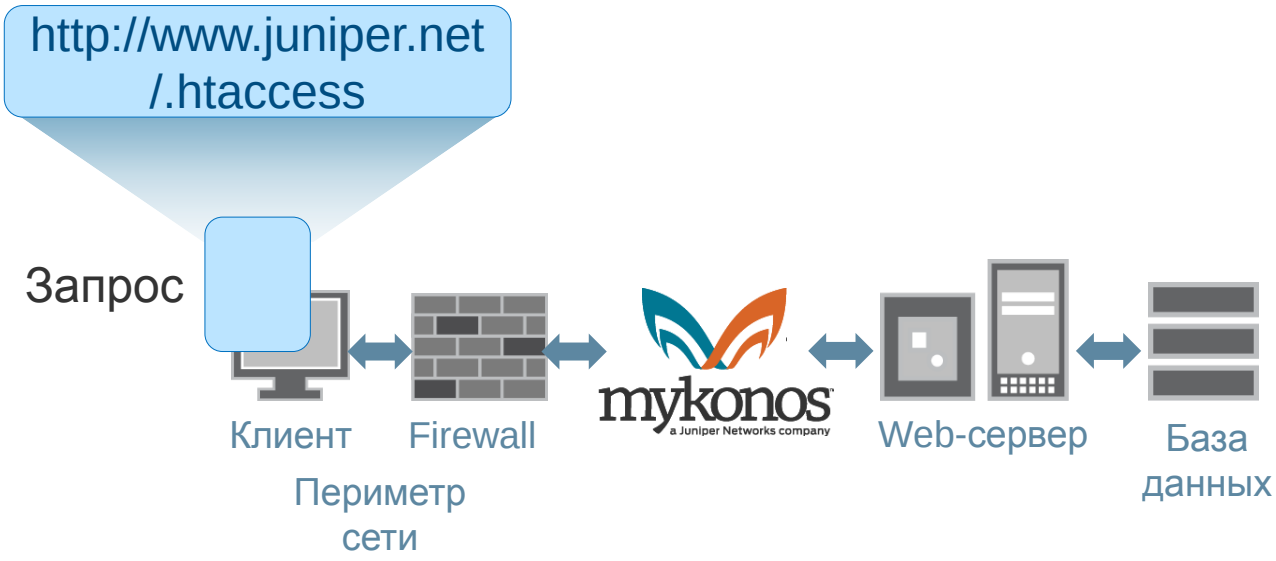


ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Добавление ловушек в код страницы

http://www.juniper.net/
?action=listing&id=2 &m4=true
<input type="hidden"…>
fake cookie "phpbsess"
fake name "Apache"

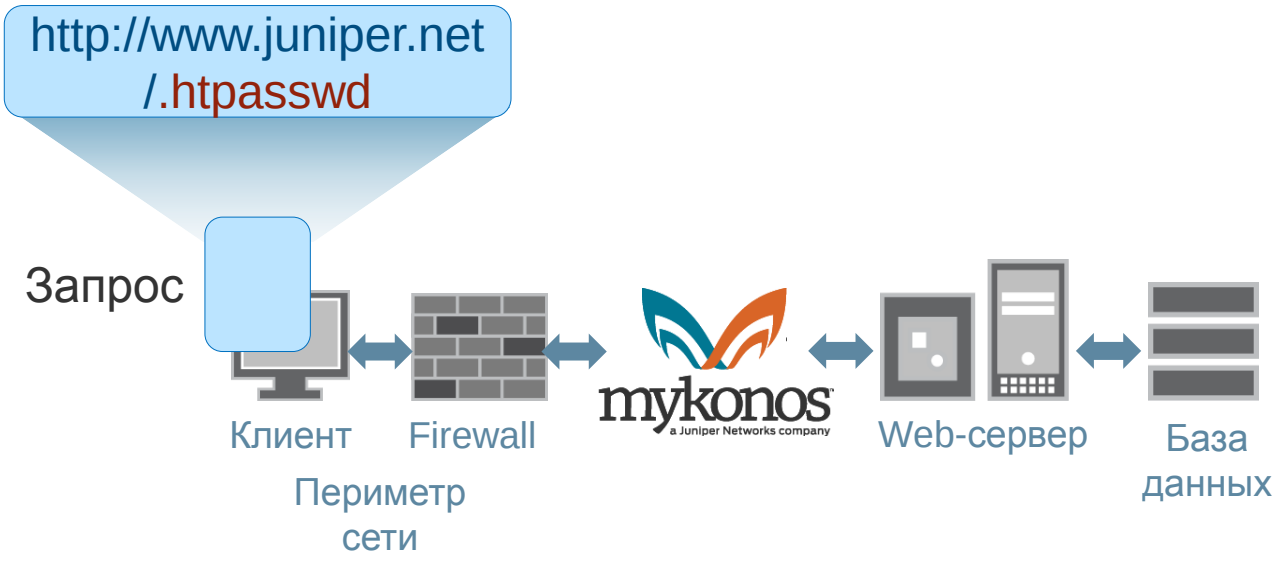
Клиент Firewall Периметр сети Web-сервер База данных

ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации



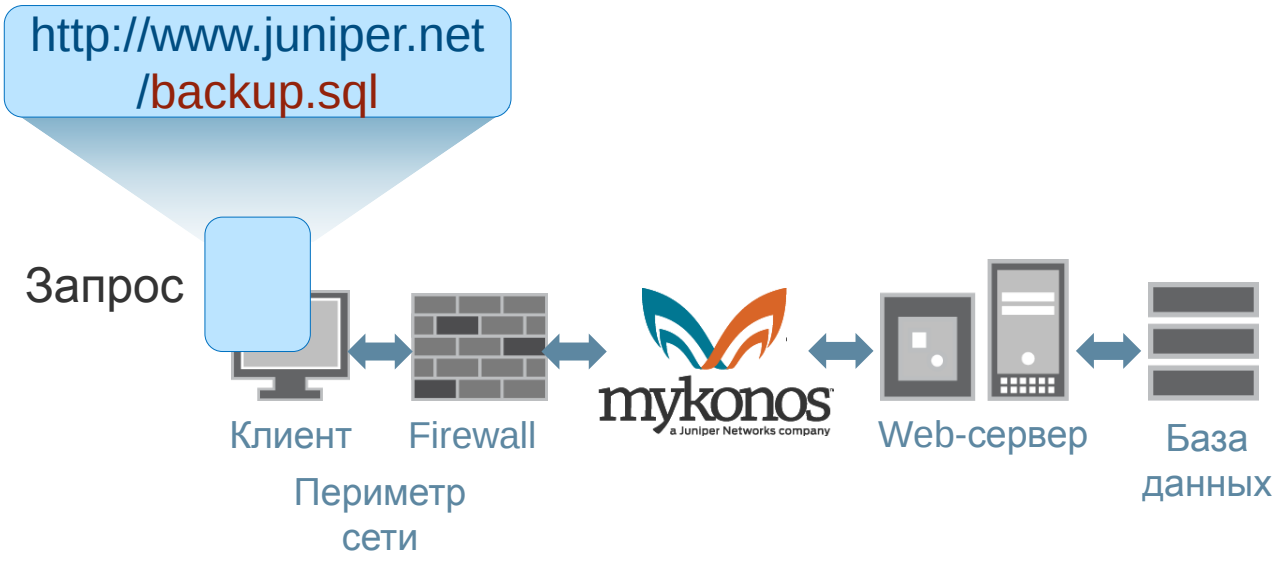
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации

ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации

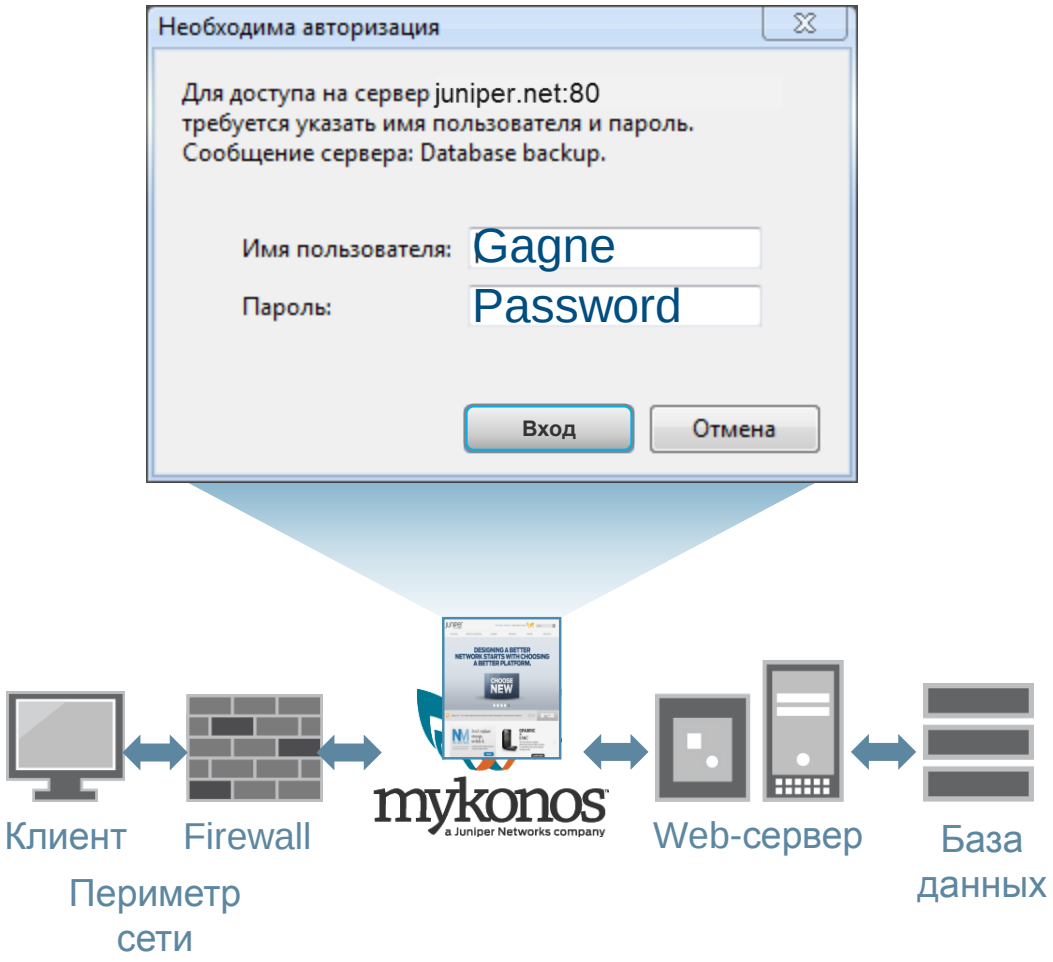


ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации

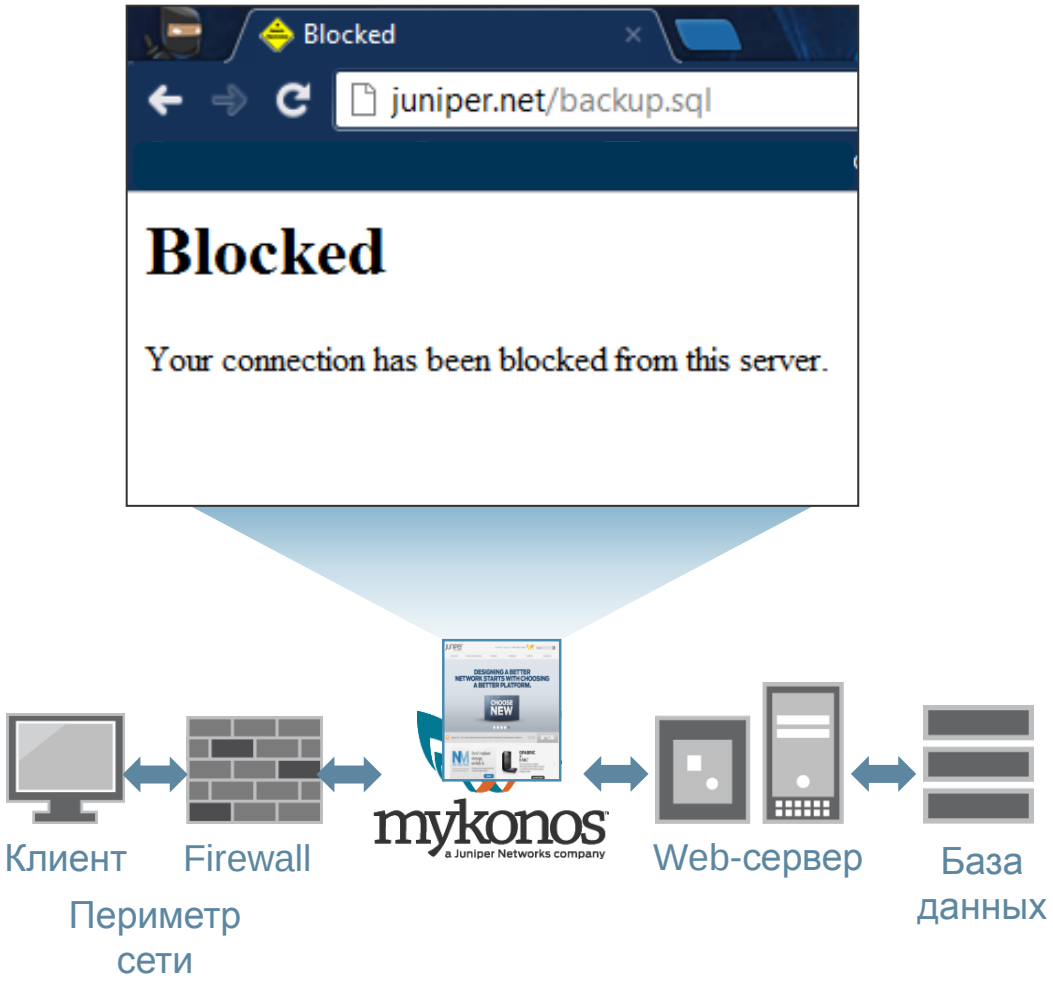
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации



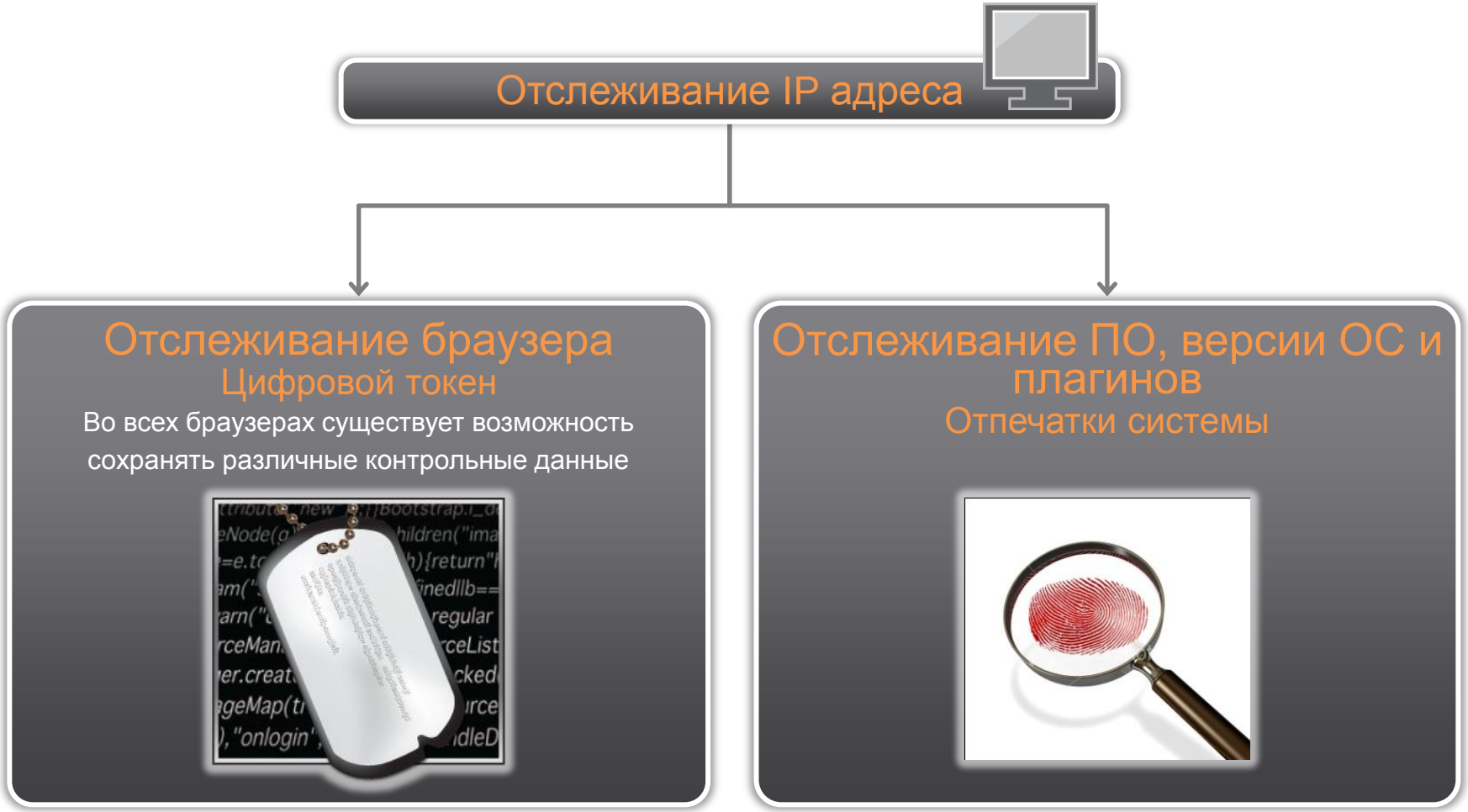
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА
Пример. Эмуляция уязвимого механизма аутентификации



ОТСЛЕЖИВАНИЕ АТАКУЮЩЕГО НЕ ТОЛЬКО ЧЕРЕЗ IP-АДРЕС



ПРИМЕР. «ОТПЕЧАТКИ» БРАУЗЕРА

Характеристики браузера	Кол-во бит идентифицирующей информации	Один из X браузеров с тем же значением	Значение
User Agent	9.84	915.84	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
Заголовки HTTP_ACCEPT	12.74	6846.06	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 windows-1251,utf-8;q=0.7,*;q=0.3 gzip,deflate,sdch ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Подробности о плагинах	1.84	3.58	no javascript
Time Zone	1.83	3.56	no javascript
Разрешение экрана и глубина цвета	1.83	3.56	no javascript
Системные шрифты	1.83	3.56	no javascript
Включены ли Cookies?	0.41	1.33	Yes
Ограниченный тест supercookie	1.83	3.56	no javascript

Данный набор параметров является **уникальным**
среди **2 500 000** аналогичных систем (https://panopticlick.eff.org)

РЕАГИРОВАНИЕ И ОБМАН ЗЛОУМЫШЛЕННИКА

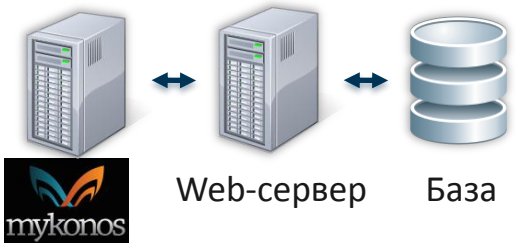
Варианты реакции MWS	Хакер, человек	Botnet	Целевое сканиро-вание	Сканиро-вание IP	Скрипты и эксплоиты
Предупреждение	●				
Блокировка	●	●	●	●	●
Ввод CAPTCHA	●	●	●	●	●
Замедление соединения	●	●	●	●	●
Симуляция сбоя приложения	●	●	●	●	●
Принудительный выход (log-out)	●	●			●

*** - Для каждого вида угроз доступны все варианты реакции. Указанные реакции наиболее уместны для указанных видов угроз**

РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY

ТРИ ТИПА ВНЕДРЕНИЯ

ПО, устанавливаемое на сервер или виртуальная машина

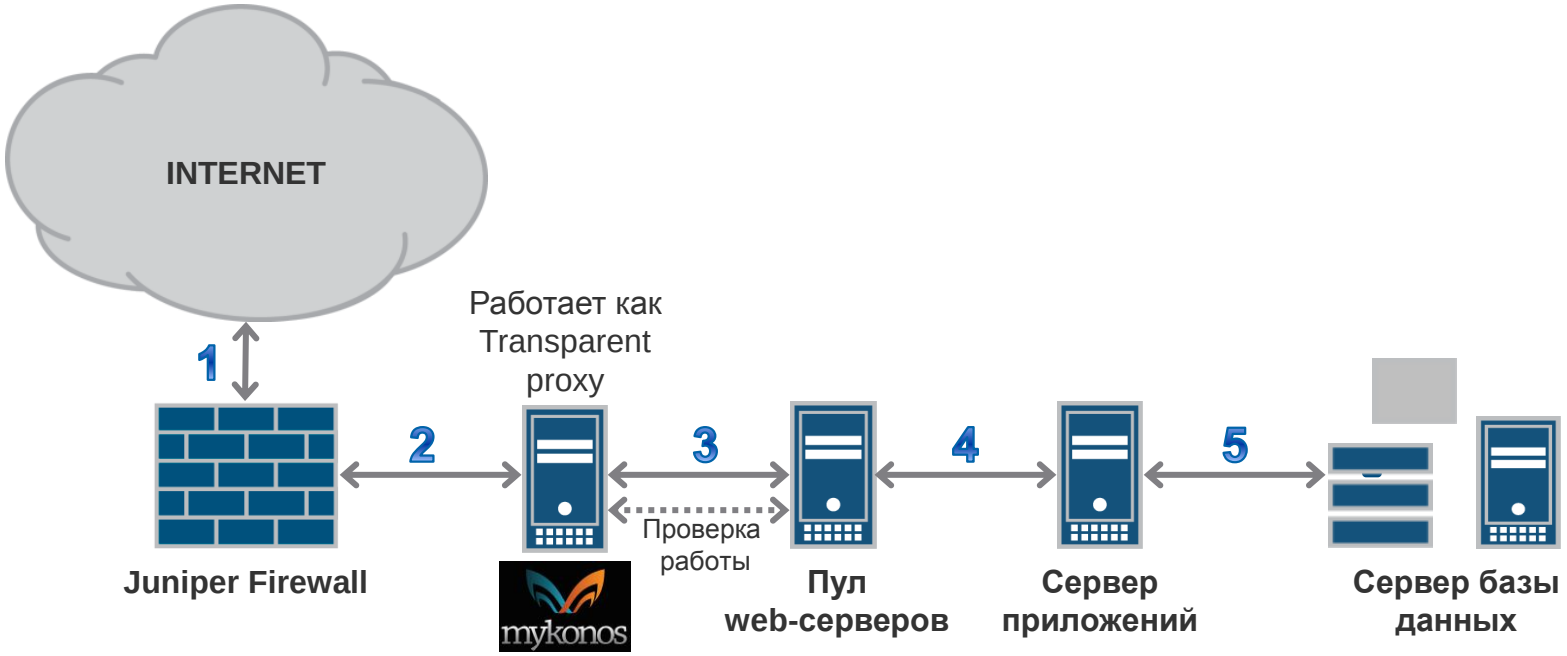


Сервер MWS1000 с преднастроенным ПО

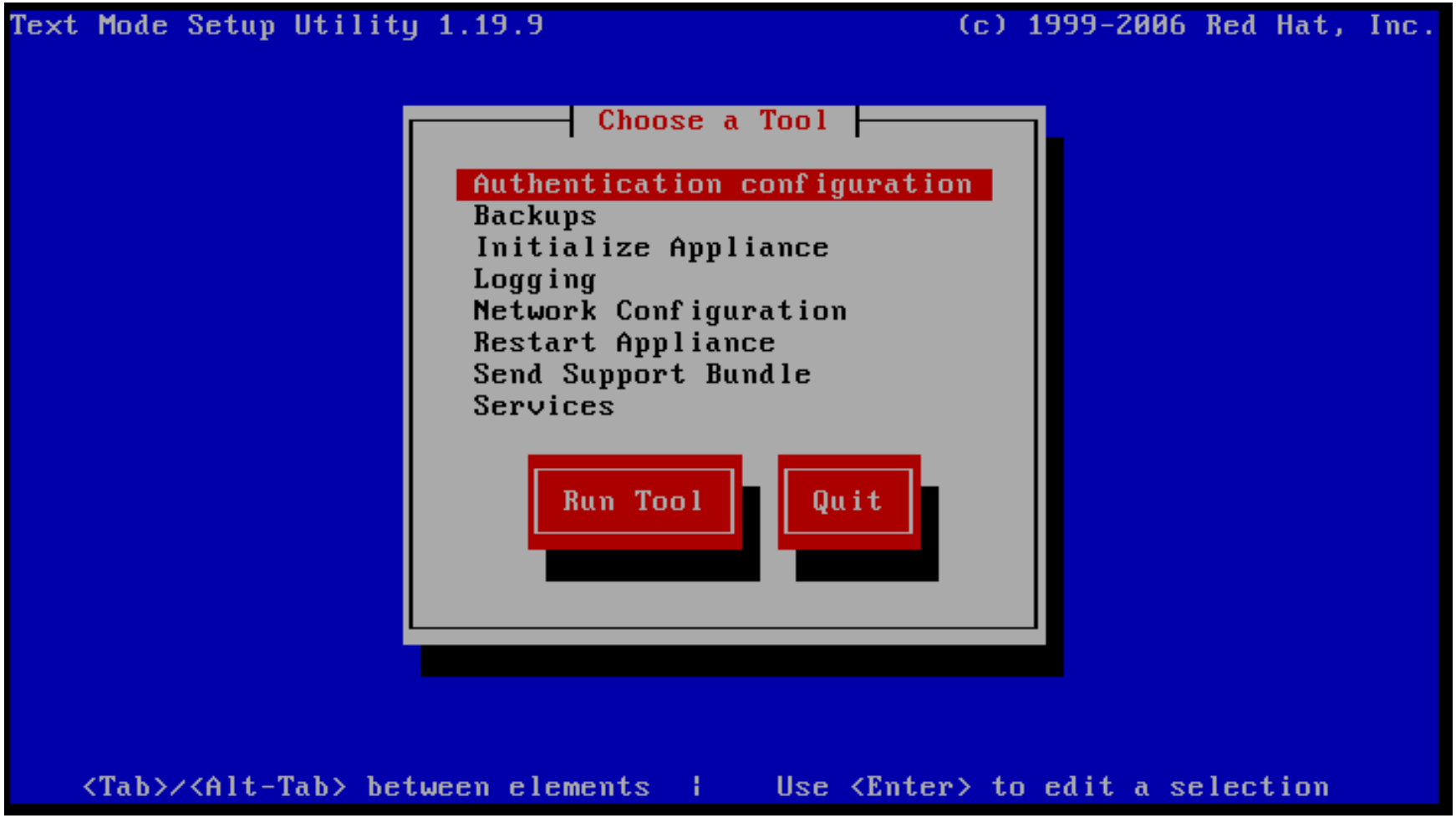
Для провайдеров услуг web-хостинга

РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY РЕЖИМ REVERSE PROXY

РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY РЕЖИМ TRANSPARENT PROXY



ИНСТАЛЛЯЦИЯ MYKONOS WEB SECURITY



ПОДРОБНОСТИ О РАБОТЕ MYKONOS WEB SECURITY

ОСНОВНЫЕ КОМПОНЕНТЫ MYKONOS

- HTTP/HTTPS прокси-шлюз

- Модуль безопасности (Security Engine) и база профилей

- Правила реагирования модуля безопасности

- Web-консоль для управления

- Программные процессоры Mykonos

ТИПЫ ПРОЦЕССОРОВ

- Процессоры Honeypot

- Процессоры обнаружения подозрительной активности

- Процессоры отслеживания атакующего

- Процессоры реагирования

ДОПОЛНИТЕЛЬНЫЕ ПОЛЕЗНЫЕ ВОЗМОЖНОСТИ

- Защита не всего ресурса, а его разделов на выбор с персональными настройками для каждого раздела

- Проверка доступности web-сервера

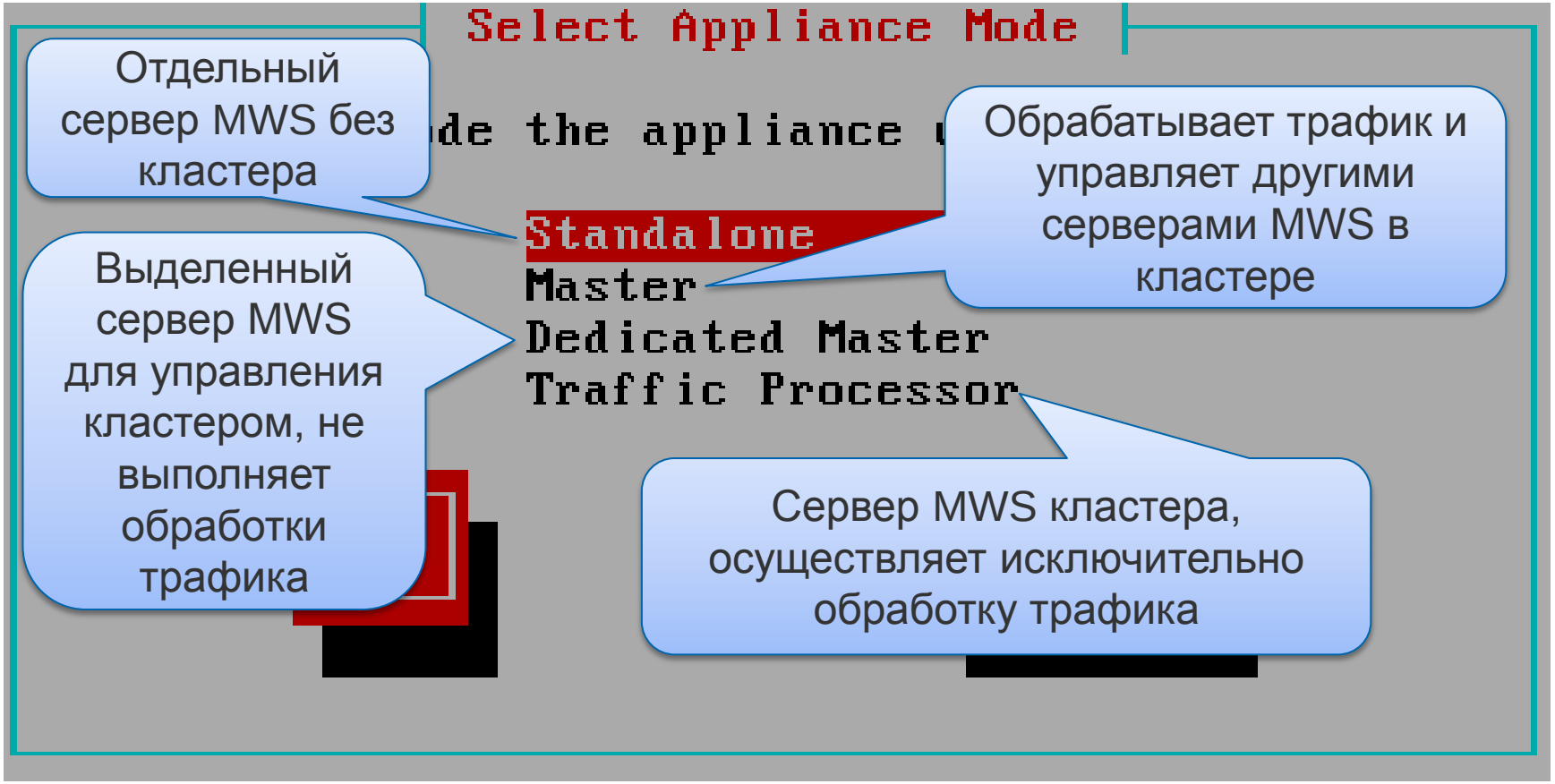
- Терминирование SSL, работа как HTTPS-прокси

- Балансировка запросов на web-серверы (комбинация round-robin, меньшего количества сессий и меньшей задержки)

- Работа в кластере для повышения производительности

КЛАСТЕР СЕРВЕРОВ MYKONOS WEB SECURITY

РОЛИ СЕРВЕРОВ MWS В КЛАСТЕРЕ

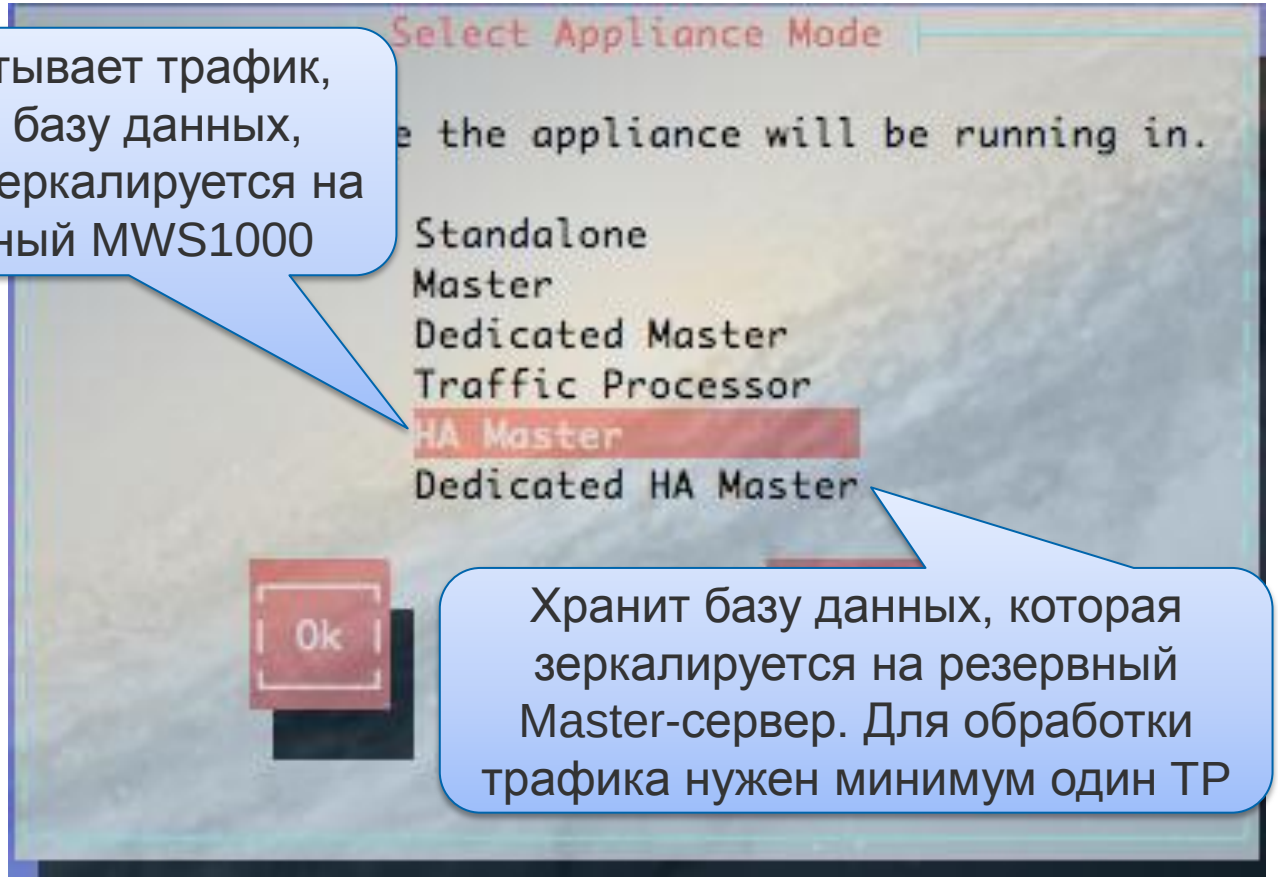


На Master и Dedicated Master располагается база данных, через них выполняется управление кластером

ОТКАЗОУСТОЙЧИВОСТЬ

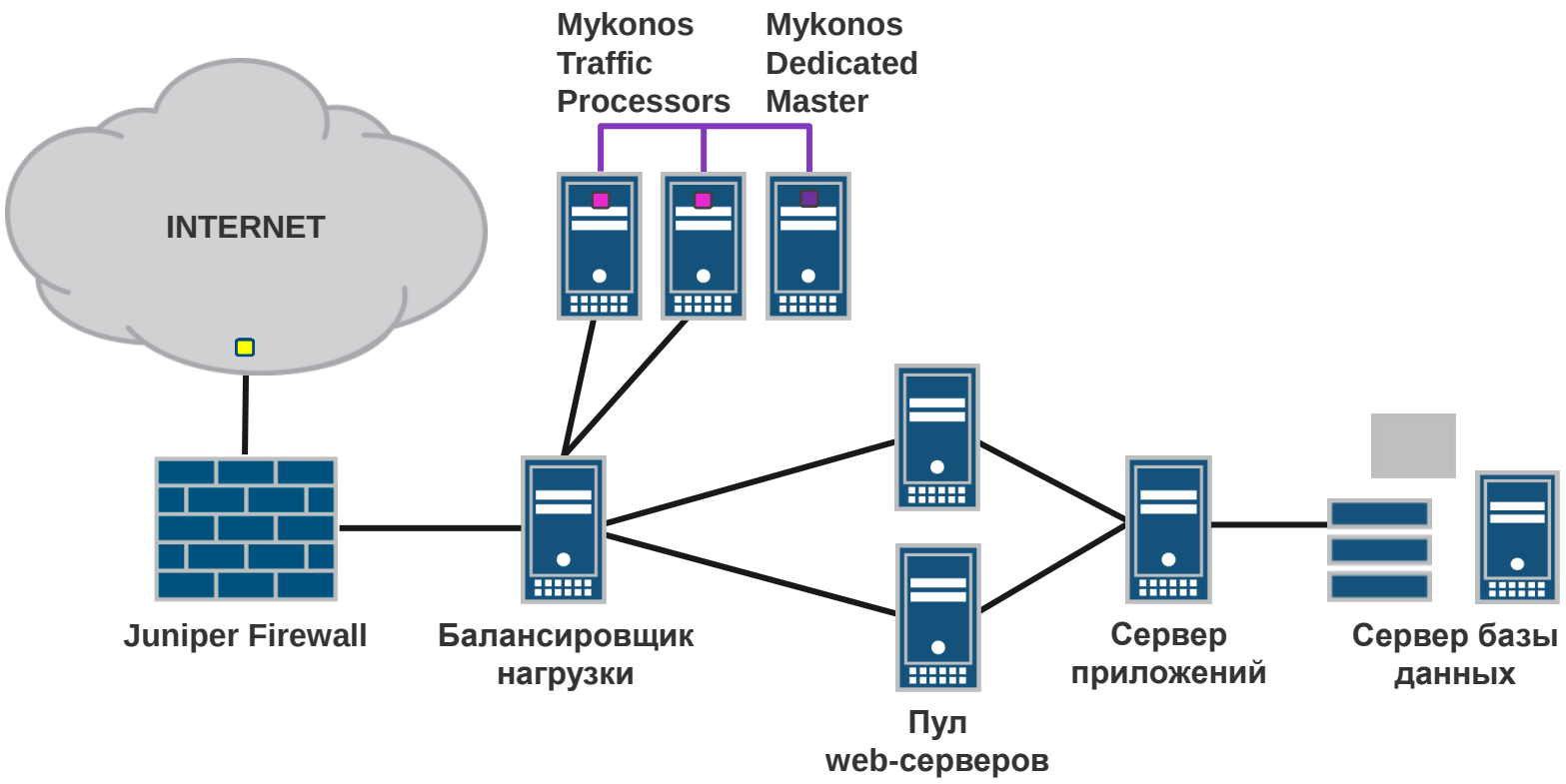
Начиная с версии 4.5 доступно создание отказоустойчивых конфигураций на базе MWS1000 (active/passive)

Обрабатывает трафик, хранит базу данных, которая зеркалируется на резервный MWS1000

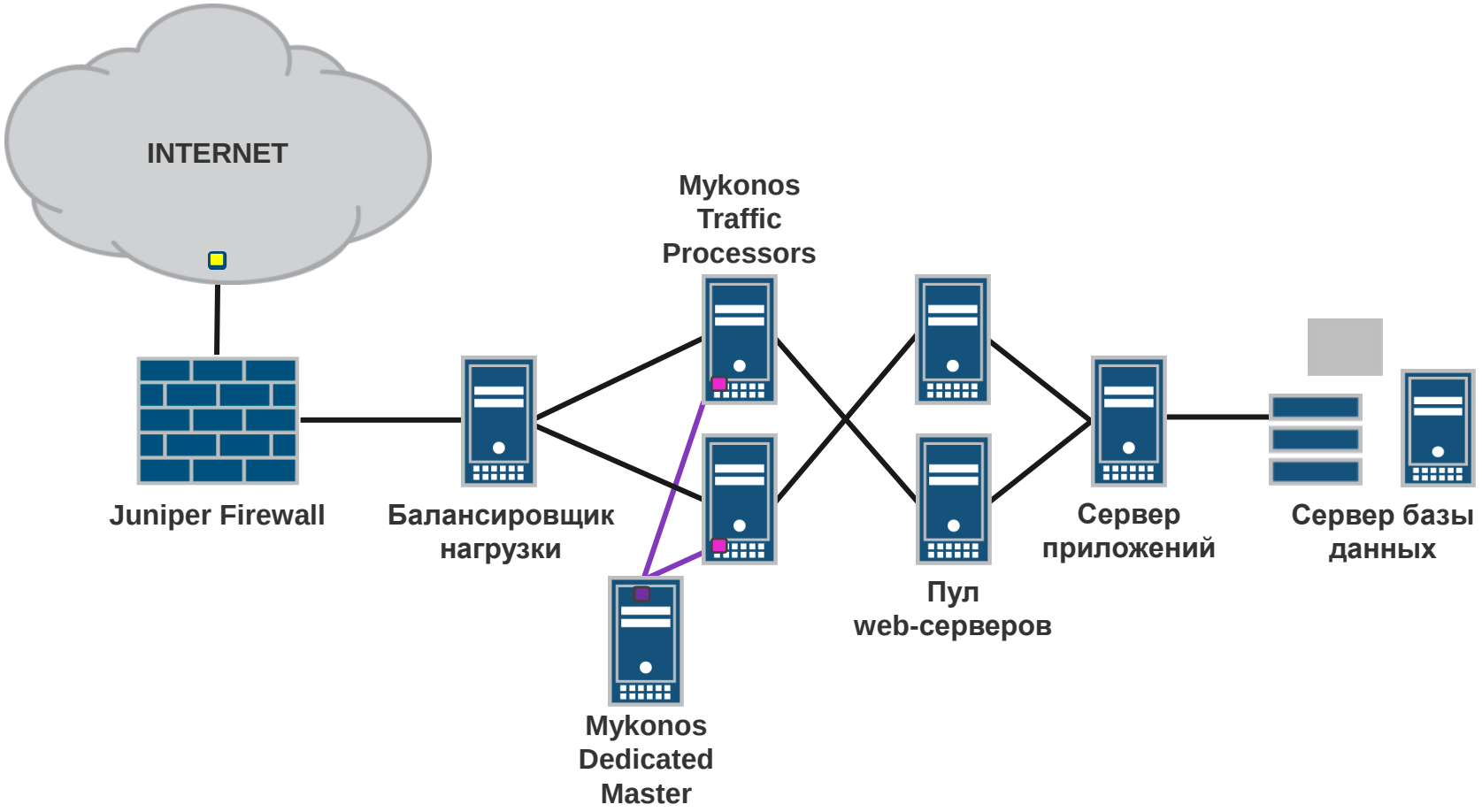


Хранит базу данных, которая зеркалируется на резервный Master-сервер. Для обработки трафика нужен минимум один TP

РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY
РАБОТА КЛАСТЕРА

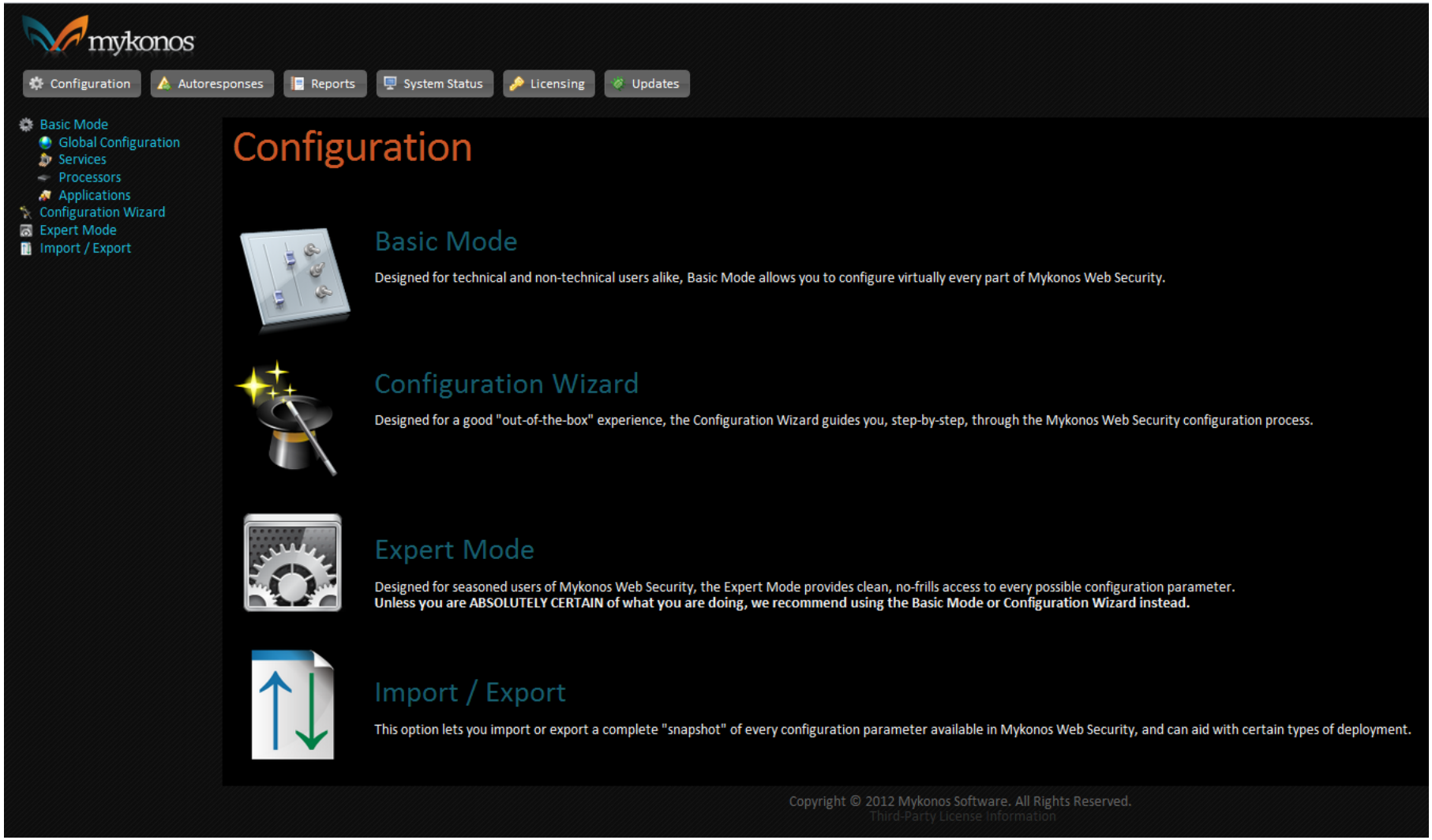


РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY
РАБОТА КЛАСТЕРА

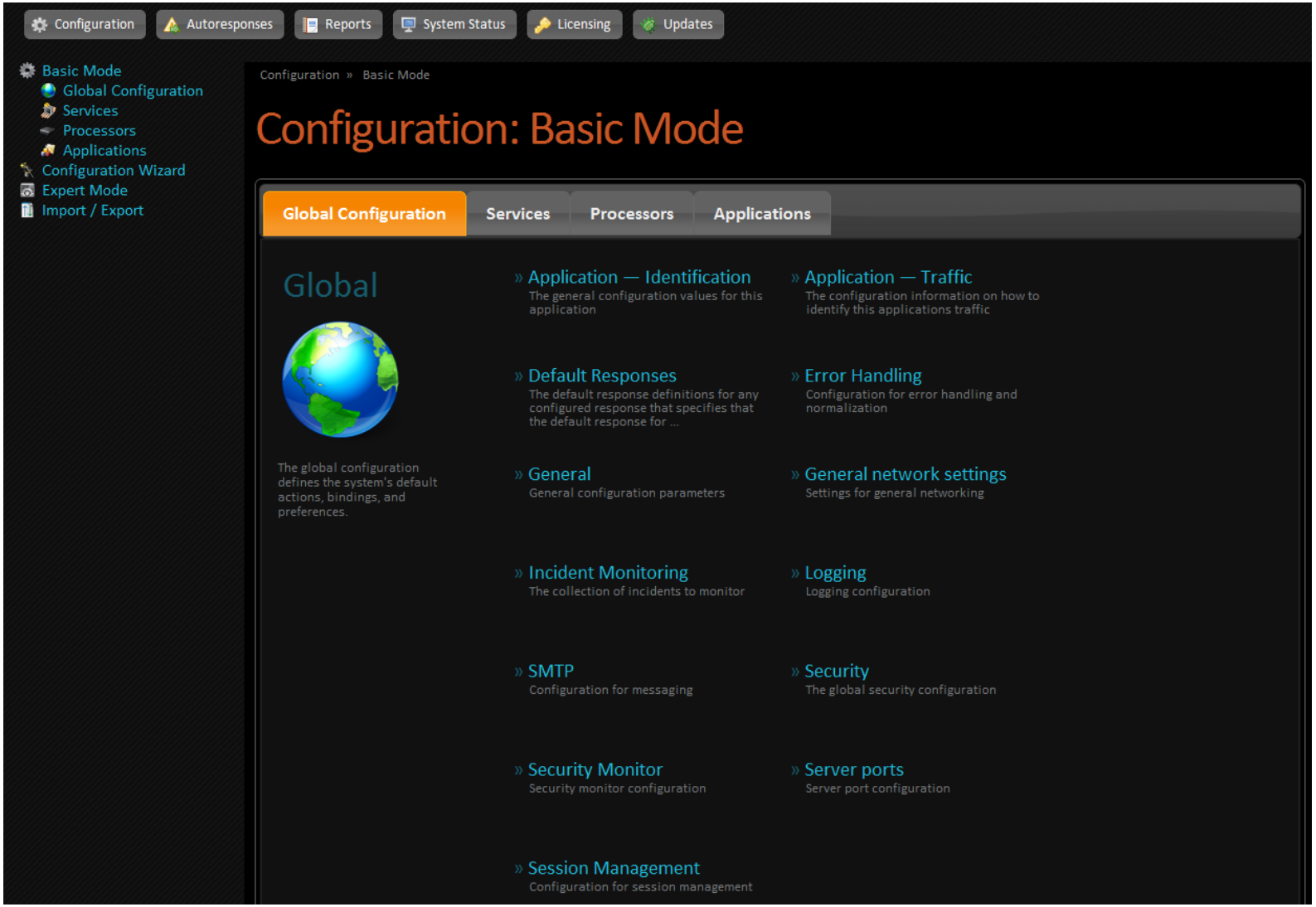


ИНТЕРФЕЙС
MYKONOS WEB SECURITY

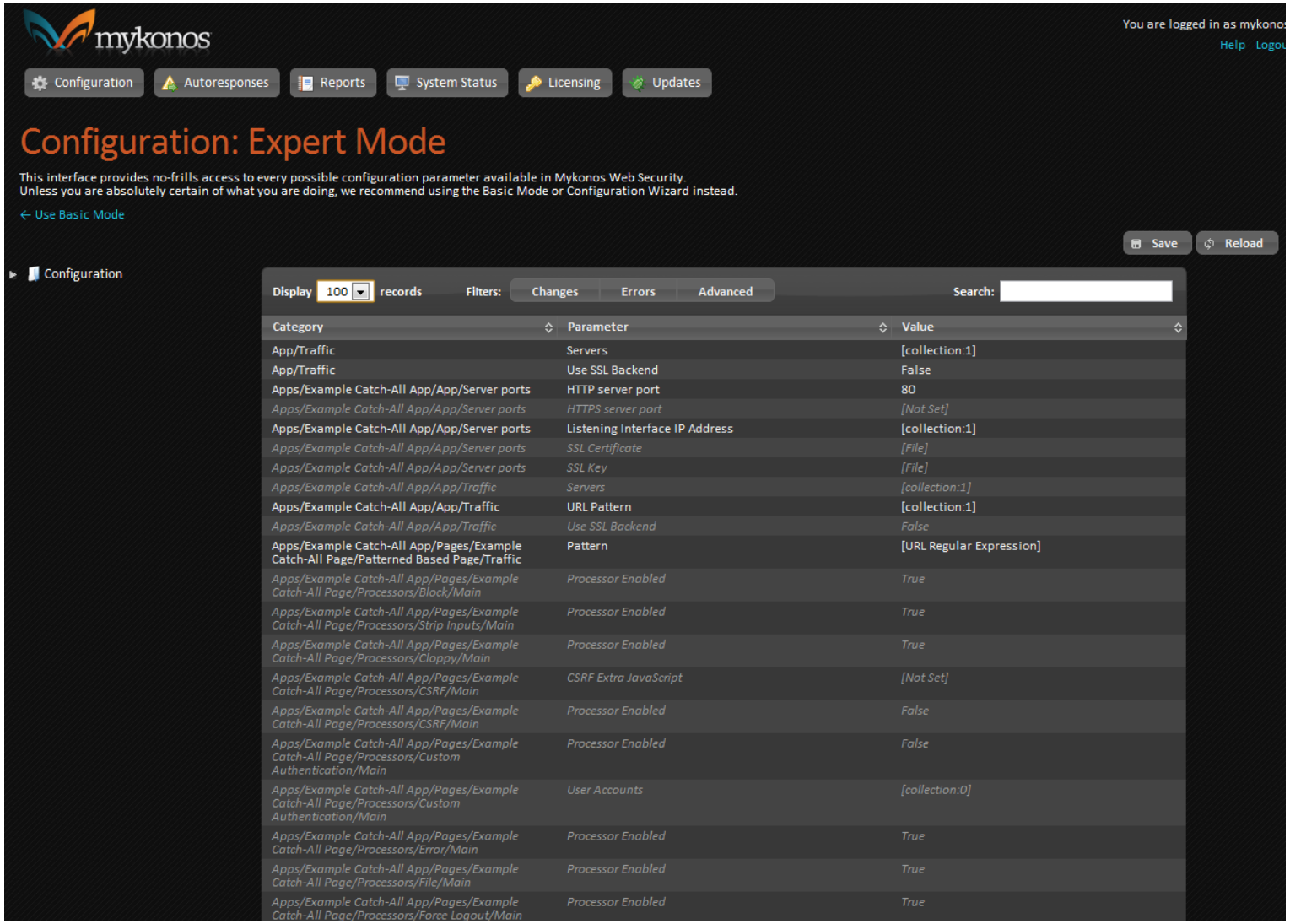
WEB-ИНТЕРФЕЙС НАСТРОЙКИ



WEB-ИНТЕРФЕЙС НАСТРОЙКИ ОСНОВНОЙ РЕЖИМ



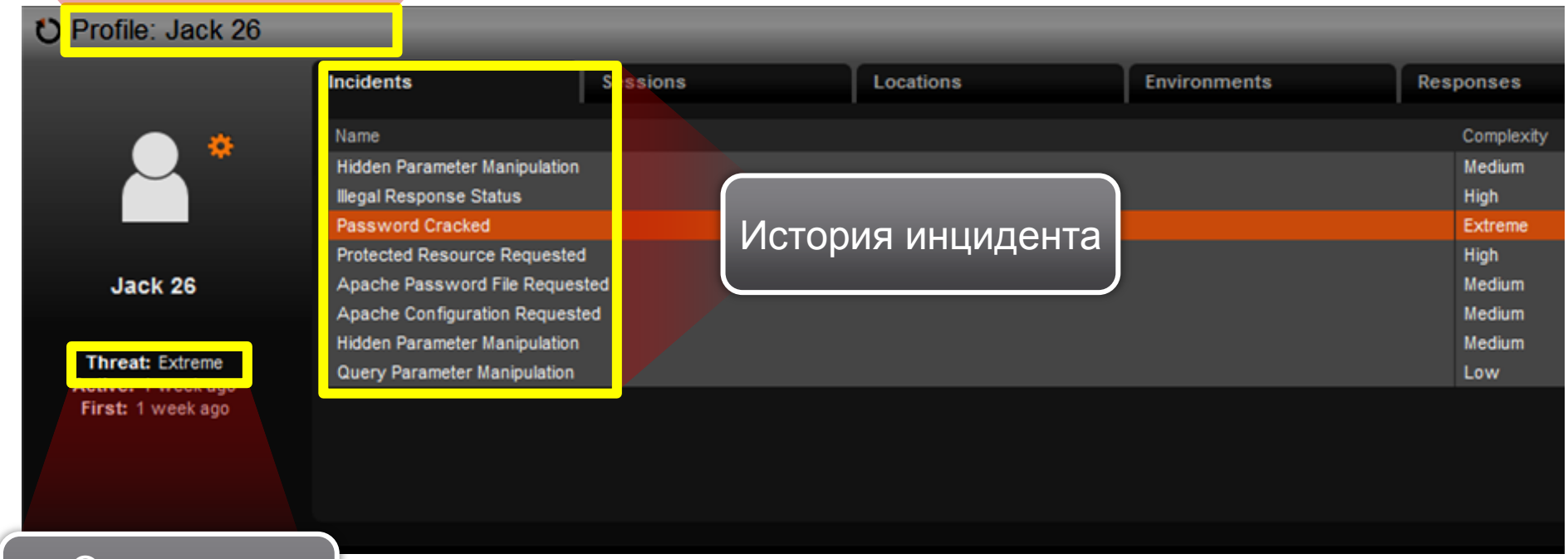
WEB-ИНТЕРФЕЙС НАСТРОЙКИ ЭКСПЕРТНЫЙ РЕЖИМ



WEB-ИНТЕРФЕЙС МОНИТОРА БЕЗОПАСНОСТИ

ПОДРОБНЫЙ ПРОФИЛЬ АТАКУЮЩЕГО

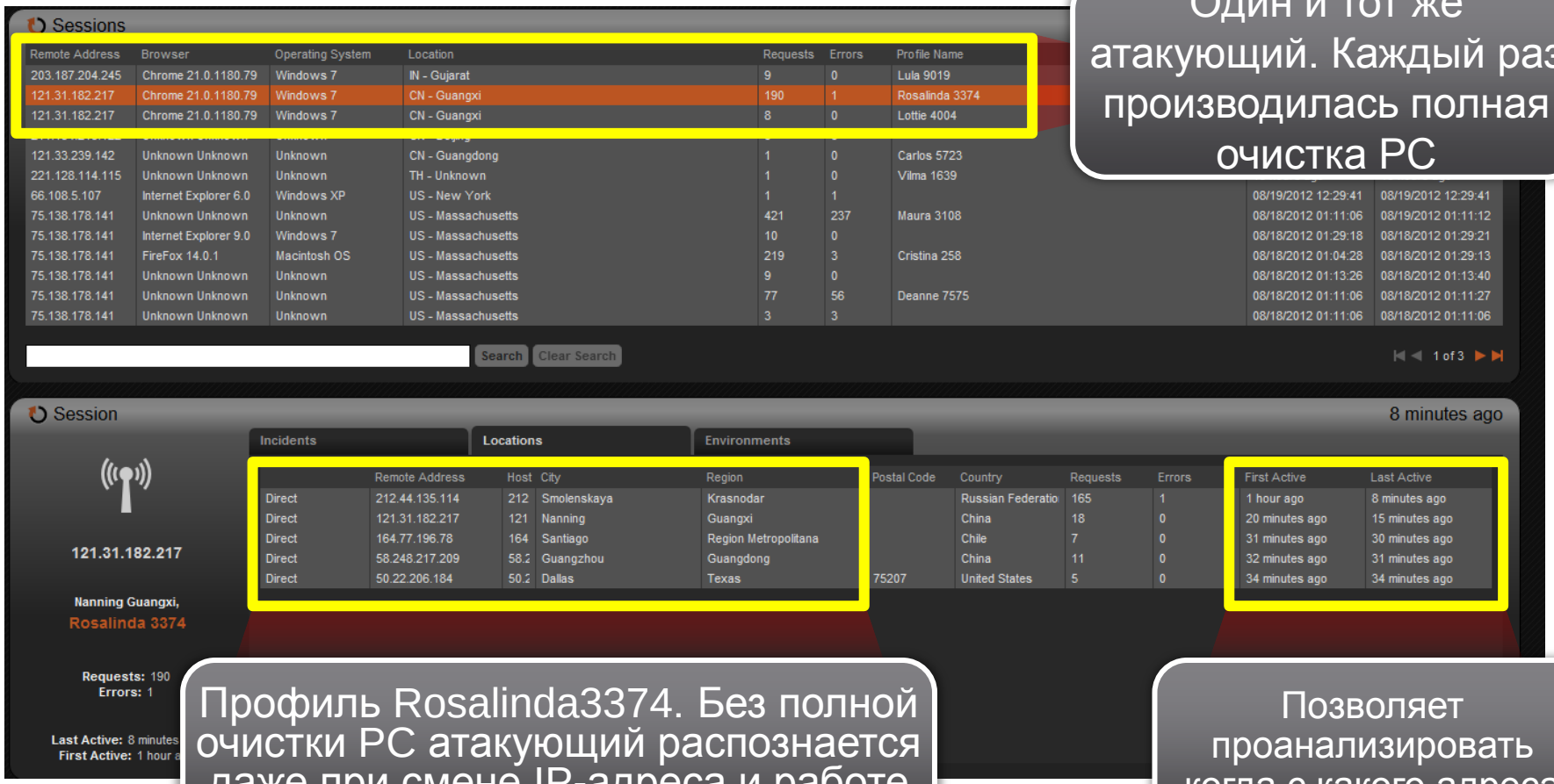
Каждому атакующему назначается имя



История инцидента

Опасность атакующего

ПРИМЕР.
ОТСЛЕЖИВАНИЕ ЗЛОУМЫШЛЕННИКА



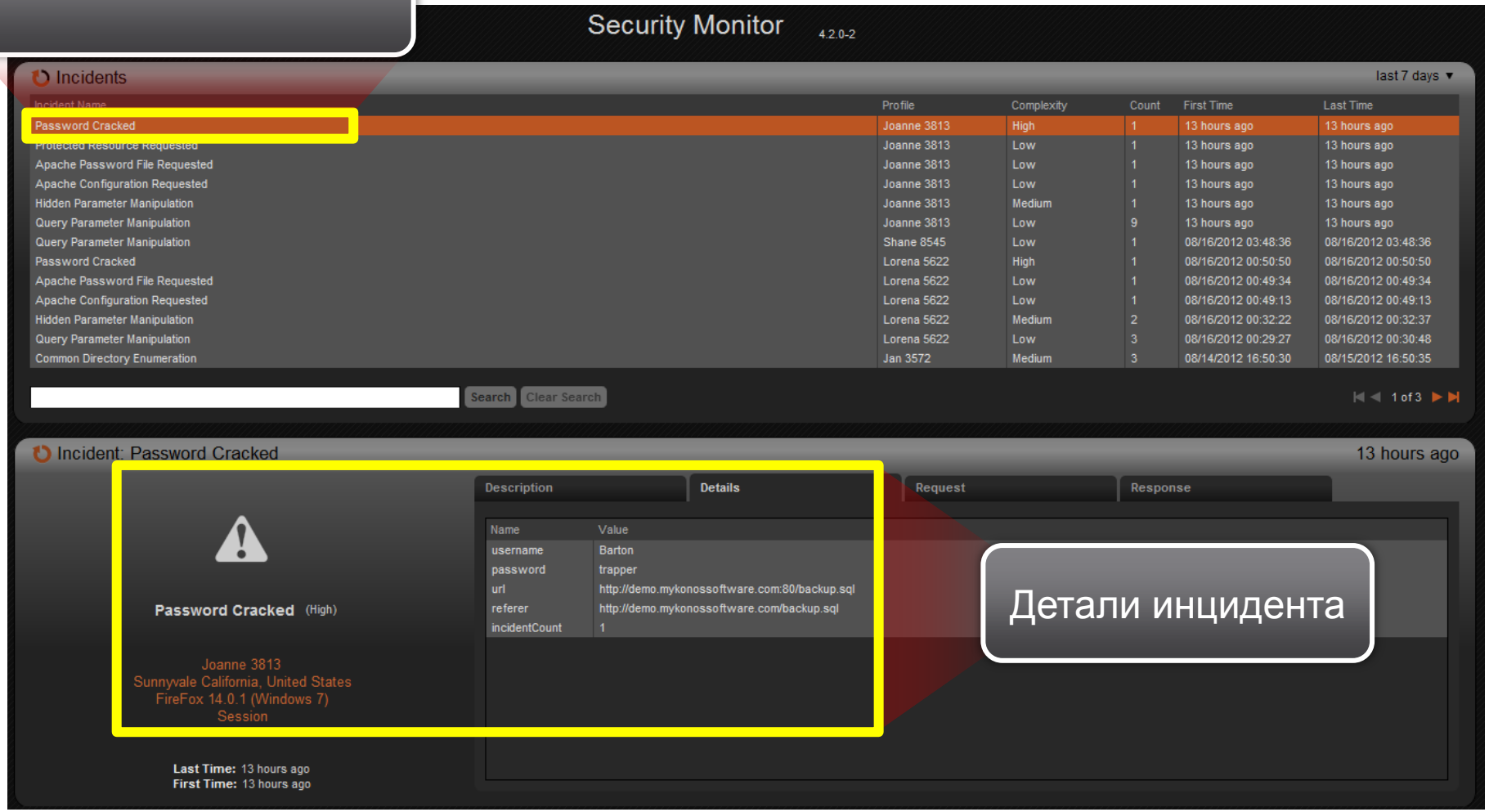
Один и тот же атакующий. Каждый раз производилась полная очистка PC

Профиль Rosalinda3374. Без полной очистки PC атакующий распознается даже при смене IP-адреса и работе через Elite proxy

Позволяет проанализировать когда с какого адреса работал атакующий

ДАННЫЕ ПО ИНЦИДЕНТУ

Выбор инцидента



Детали инцидента

ПРИМЕРЫ ОТЧЕТОВ

Incident Detail for 66.129.224.36 from 01-Aug-12 00:00 to 14-A

Created	User Agent	Request Content	Response Content
03-Aug-12 11:11	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)	POST /?action=cart HTTP/1.1 host: demo.mykonossoftware.com x-forwarded-for: 66.129.224.36 x-myk-request-info: http, HTTP/1.1, 80 x-myk-appid: 171544 x-myk-port: 80 x-myk-use-ssl: false x-myk-ssl: false connection: close user-agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1 accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 accept-language: en-us,en;q=0.5 accept-encoding: gzip, deflate referer: http://demo.mykonossoftware.com/?action=cart cookie: PHPSESSID=ltu99ofqjt2huoguhlup6mfmr0; PHPSESSID_s=0438cd02a223e3a98db530745ae6bca content-type: application/x-www-form-urlencoded content-length: 28 x-myk-access-log-id: CE2CB95E-97C0-4A99-8CE8-82997ED1A913 qt_2=1	HTTP/1.1 200 OK Date: Fri, 03 Aug 2012 15:11:45 GMT Content-Type: text/html; charset=UTF-8 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-rev Pragma: no-cache Server: Microsoft IIS Content-length: 8864 <!DOCTYPE HTML PUBLIC "-//W3C//DTD H org/TR/html4/strict.dtd"> <html> <head> <title>Generic Electronics</title> <meta http-equ text/html; charset=UTF-8"> <link rel="SHO <link rel="style type="text/css"> <link rel="style text/css"> <script type=" ></script><script type="text/javascript" src=" type="text/javascript" src="/9LpZNC9GXCqu ></script> </head> <body> <div class="sit
03-Aug-12 11:11	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)	POST /?action=cart HTTP/1.1 host: demo.mykonossoftware.com x-forwarded-for: 66.129.224.36 x-myk-request-info: http, HTTP/1.1, 80 x-myk-appid: 171544 x-myk-port: 80 x-myk-use-ssl: false x-myk-ssl: false connection: close user-agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1 accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 accept-language: en-us,en;q=0.5 accept-encoding: gzip, deflate referer: http://demo.mykonossoftware.com/?action=cart cookie: PHPSESSID=ltu99ofqjt2huoguhlup6mfmr0; PHPSESSID_s=0438cd02a223e3a98db530745ae6bca content-type: application/x-www-form-urlencoded content-length: 29 x-myk-access-log-id: 6053CE9A-8169-4B03-3C2C-456ED4BEF502 qt_2=1	HTTP/1.1 200 OK Date: Fri, 03 Aug 2012 15:12:00 GMT Content-Type: text/html; charset=UTF-8 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-rev Pragma: no-cache Server: Microsoft IIS Content-length: 8864 <!DOCTYPE HTML PUBLIC "-//W3C//DTD H org/TR/html4/strict.dtd"> <html> <head> <title>Generic Electronics</title> <meta http-equ text/html; charset=UTF-8"> <link rel="SHO <link rel="style type="text/css"> <link rel="style text/css"> <script type=" ></script><script type="text/javascript" src=" type="text/javascript" src="/9LpZNC9GXCqu ></script> </head> <body> <div class="sit

Детализация инцидентов по IP-адресу

Hacker Detection & Prevention Scorecard

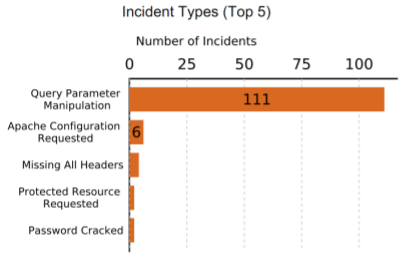
Mykonos System Report

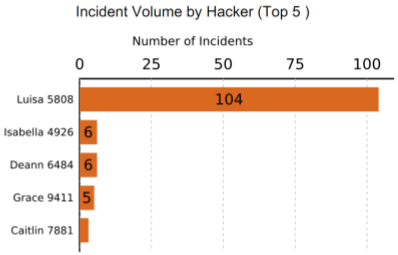
http://www.mykonossoftware.com/

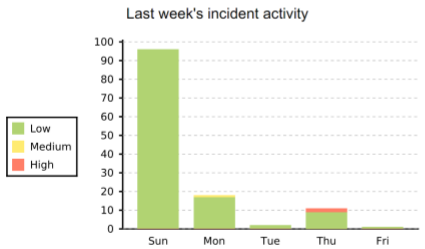
05-Aug-12 to 11-Aug-12

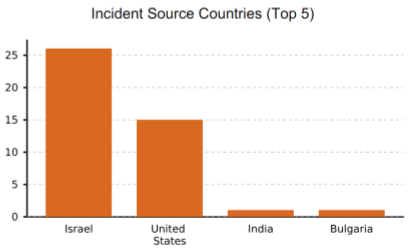
Executive Summary

	Attackers Detected	Attackers Blocked	Incidents detected
Since Deployment (19-Apr-12 to 17-Aug-12)	182	46	5530
Last Month (01-Jul-12 to 31-Jul-12)	52	18	971
Last Week (05-Aug-12 to 11-Aug-12)	9	2	128









Weekly Report

Threat level of Attackers	Low	Medium	High	Total
Number of Attackers	6	1	2	9

Responses Deployed	Blocking	Non-blocking	None	Total
Number of Responses	2	17	0	19

Обобщенные данные

ПРОИЗВОДИТЕЛЬНОСТЬ

Характеристики MWS1000:

- Dual Intel Quad Core (2.4GHz) CPU, 48GB RAM, 4 x GE NIC, 2 x SFP+ 10GE (optional), 1RU

Пример:

Сервер Dell R200 (dual core 3Ghz, 4GB RAM, 1 SAS 5400 rpm HDD):

- 1 сервер – 250 Мбит/с
- 1 мастер + 1 TP – 311 Мбит/с, 4500 запросов/с (+30%)
- 1 мастер + 2 TP – 420 Мбит/с, 6600 запросов/с (+30%)
- 1 мастер + 3 TP – 630 Мбит/с, 9200 запросов/с (+50%)
- 1 мастер + 4 TP – 830 Мбит/с, 12000 запросов/с (+30%)

Средняя задержка – 5…40мс

ЗАКАЗ

Программно-аппаратный комплекс MWS1000:

MWS1000	Mykonos Web Security Hardware Appliance – SW Sold Separately	$40 000
MWS100MB	Mykonos Web Security 100Mbps Licenses	$25 000
Поддержка	Поддержка MWS1000	---
SVC-COR-MWS100MB	Juniper Care Core Support for MWS100MB	$5 500

ISO-образ или VM, подписка на 1 или 3 года:

MWS-SL-1	Mykonos MWS Software - 100Mbps for one geographic site. Including support and updates. One year term	$17 500
MWS-SL-3	Mykonos MWS Software - 100Mbps for one geographic site. Including support and updates. Three year term	$47 250

everywhere