

MYKONOS

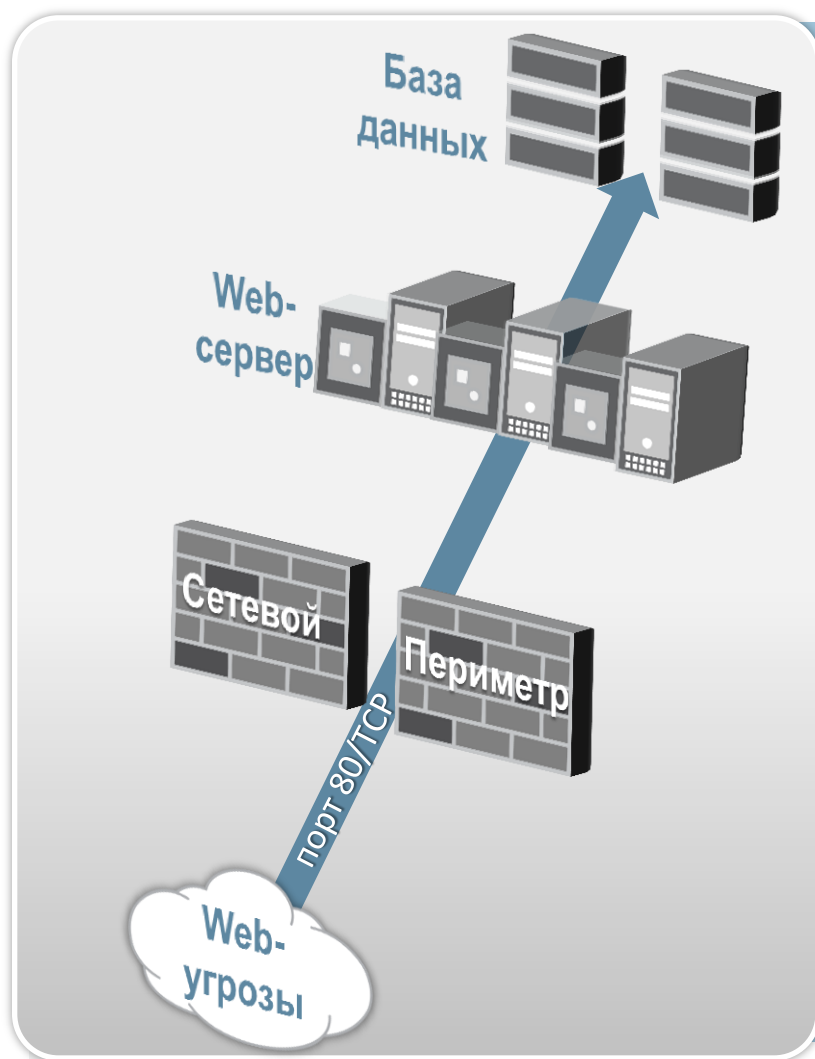
ЛУЧШИЙ СПОСОБ ЗАЩИТИТЬ ВАШ WEB-САЙТ И
WEB-ПРИЛОЖЕНИЕ ОТ АТАК

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

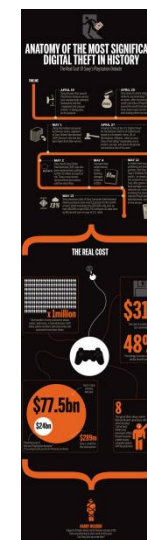
Sony
Судебные издержки
\$1-2 млрд.

Ухудшение
репутации

Снижение
доходов

Прямые издержки
Sony
\$171 млн.

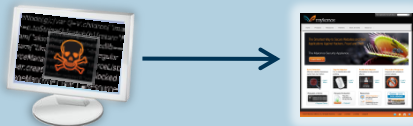
- 23 дня простоя сети
- Потеря заказчиков



УГРОЗЫ, ИСХОДЯЩИЕ ОТ ХАКЕРОВ

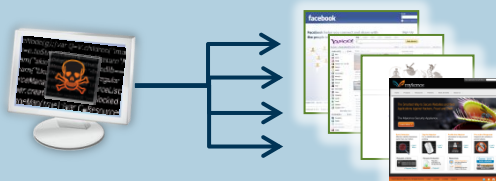
Скрипты & Эксплоиты

Общие скрипты и инструменты хакеров



IP-сканирование

Поиск определенных уязвимостей при помощи скриптов на многих сайтах



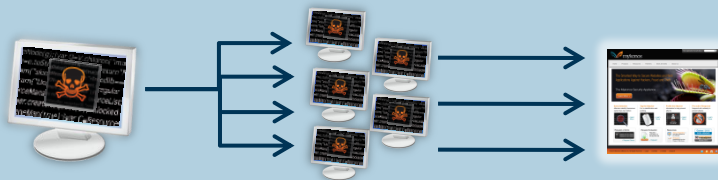
Целевое сканирование

Поиск уязвимостей определенного сайта



Ботнеты

Скрипты выполняются зараженными машинами и осуществляют атаку



Высококвалифицированные хакеры

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



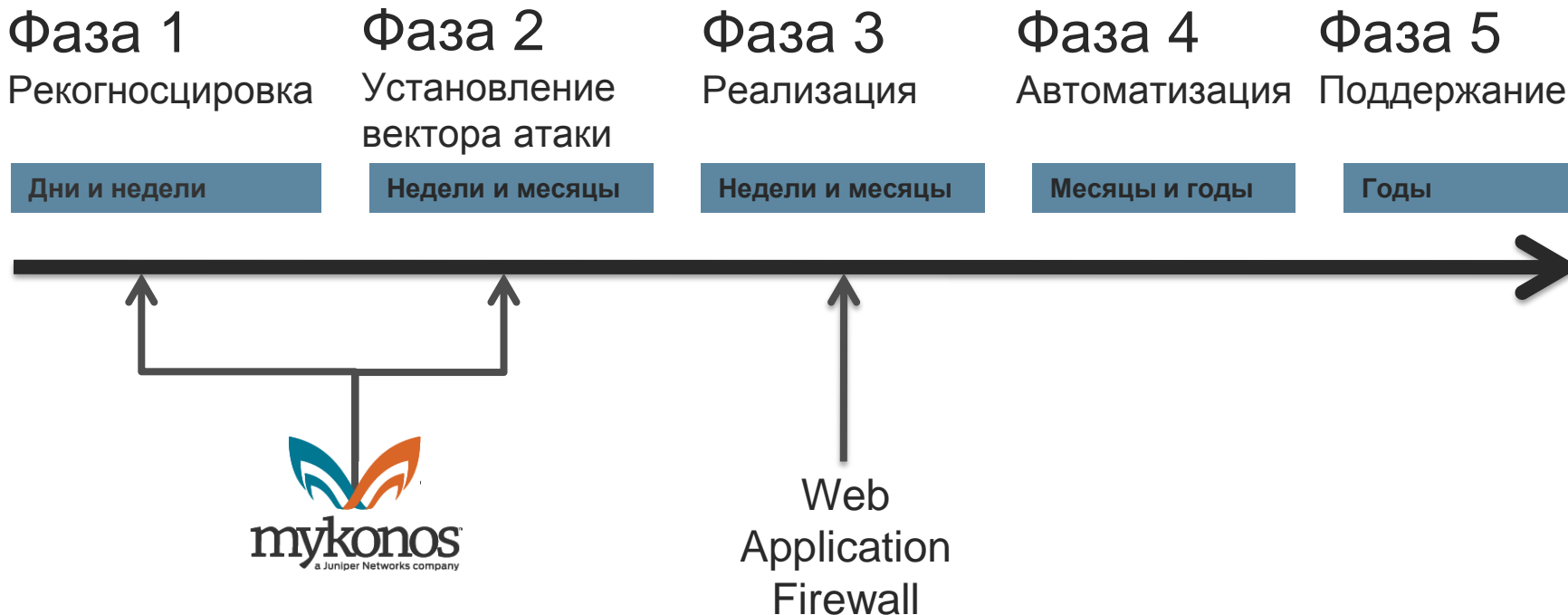
ОБЩИЕ ДАННЫЕ О MYKONOS WEB SECURITY

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

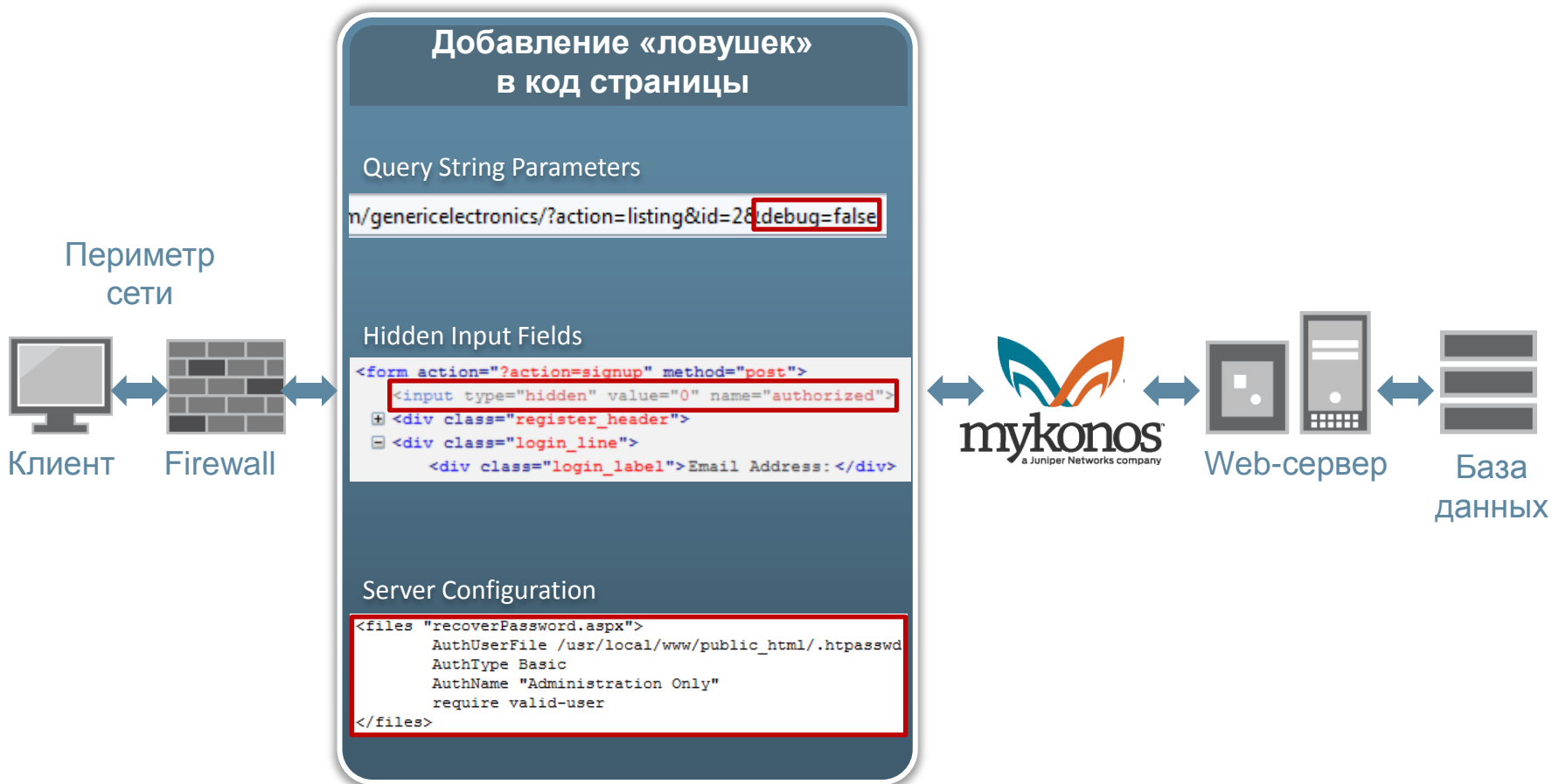
Понимание возможностей и намерений атакующего



Реагирование

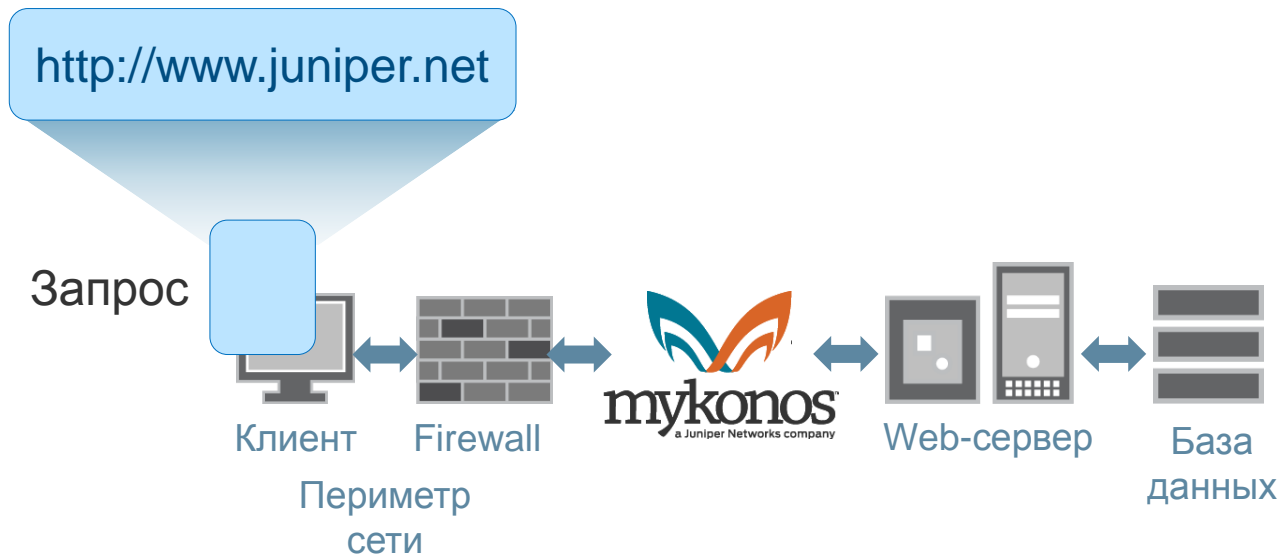
Адаптивная реакция, включающая блокировку предупреждение и обман

ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА



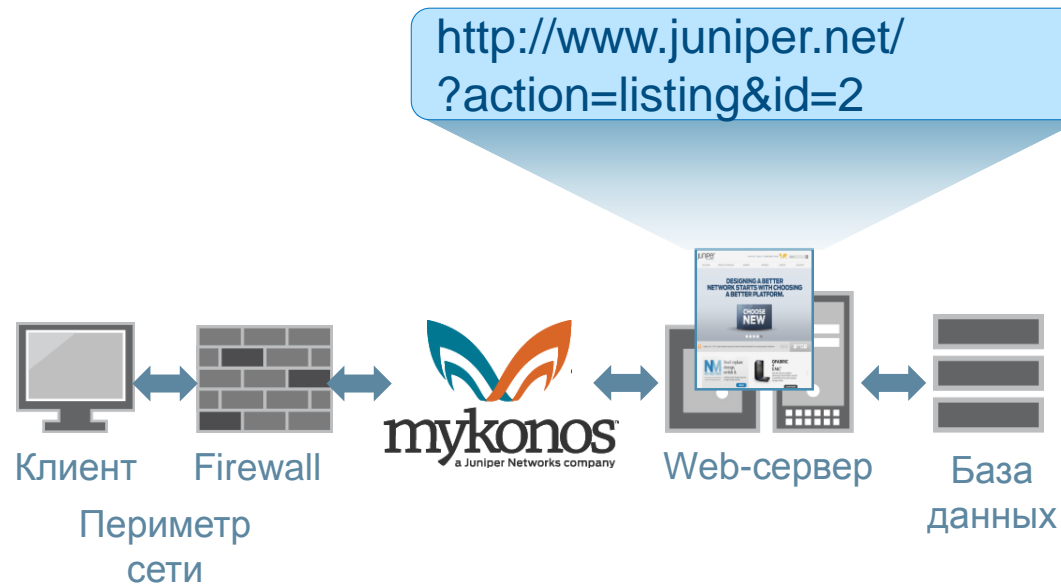
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Добавление ловушек в код страницы



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Добавление ловушек в код страницы



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

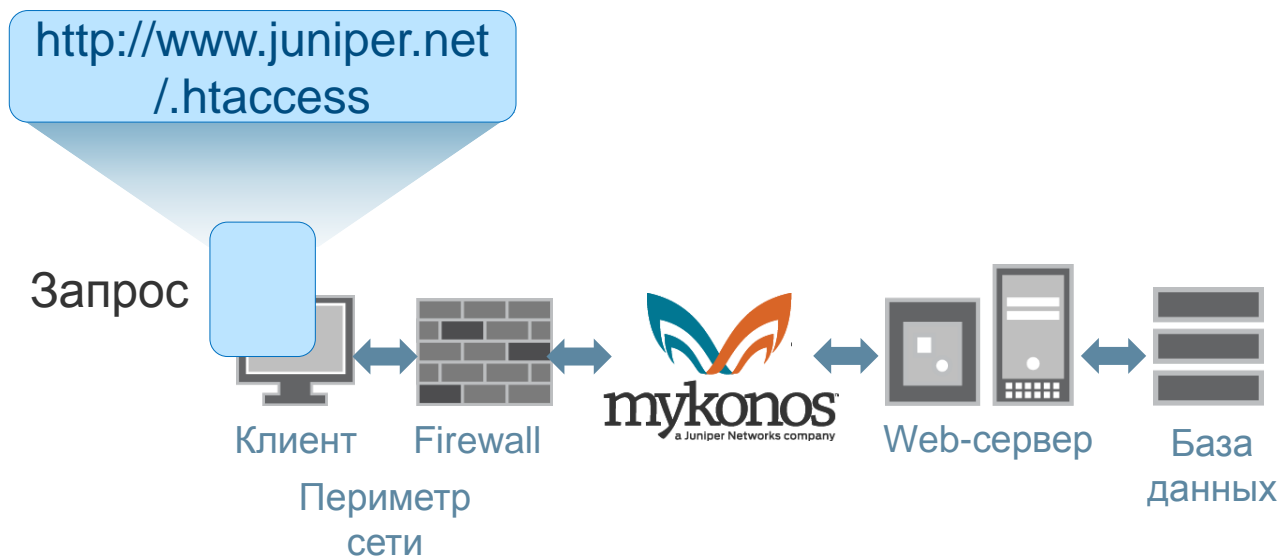
Добавление ловушек в код страницы

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



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации

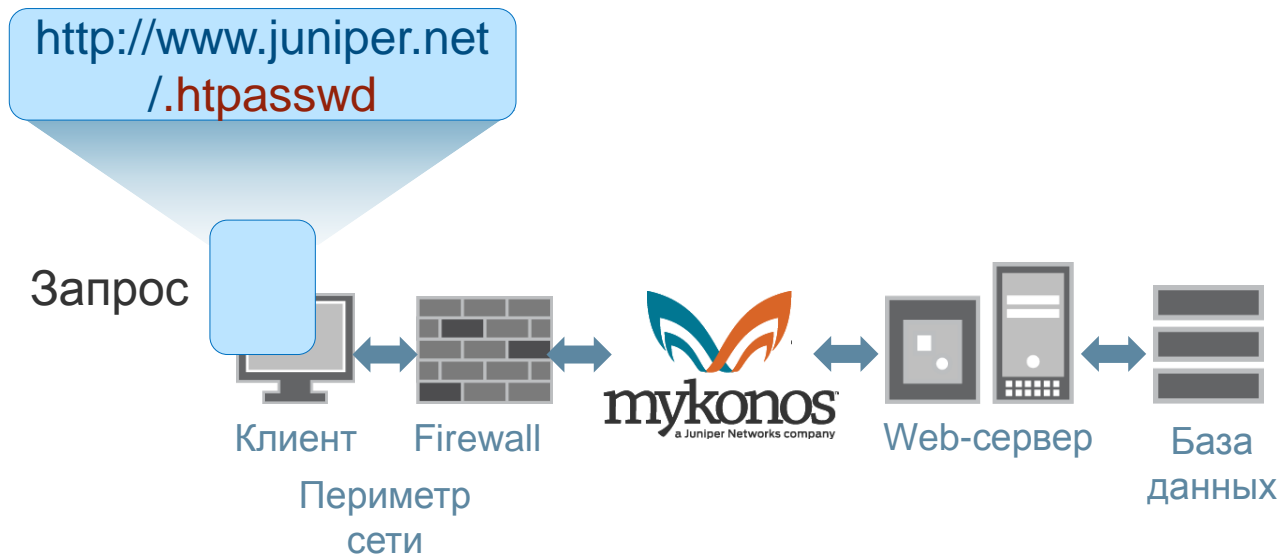
Ложный ответ

```
<files "backup.sql">  
AuthUserFile /www/root/.htpasswd  
AuthType Basic  
AuthName "Database backup"  
require valid-user  
</files>
```



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации

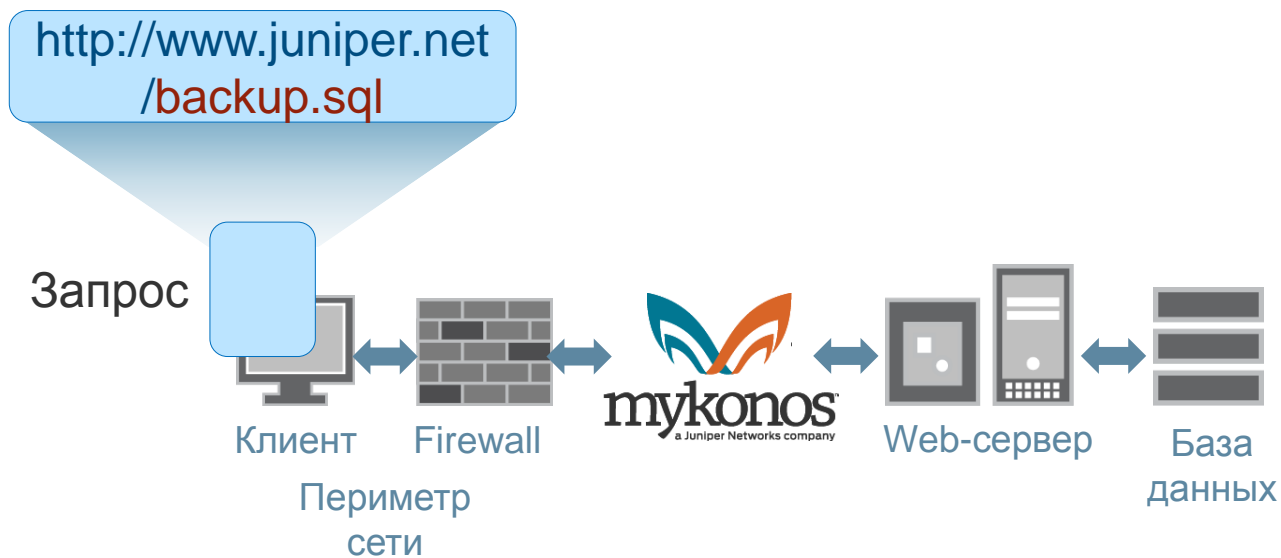
Ложный ответ

kostenba:d8HYPcCGtdMWw
Gagne:fhAOHA3cP9Nhc
ehganm:wydEzOpLi9urc
Robt-CCN:8k6Ef1MvjLnp2
Barton:1Zssf1HtwMFxk
bengay:xbwCbfeX7ZrZQ



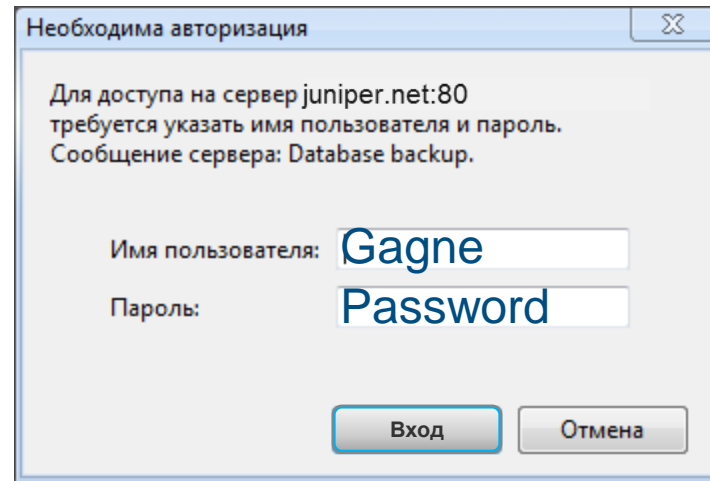
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации



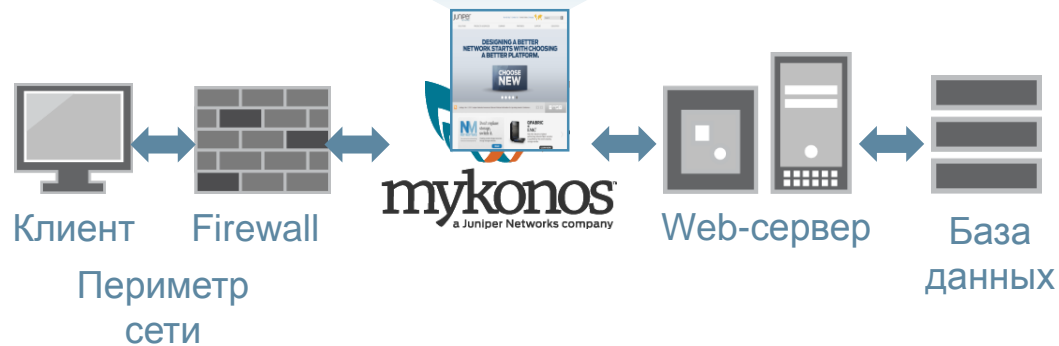
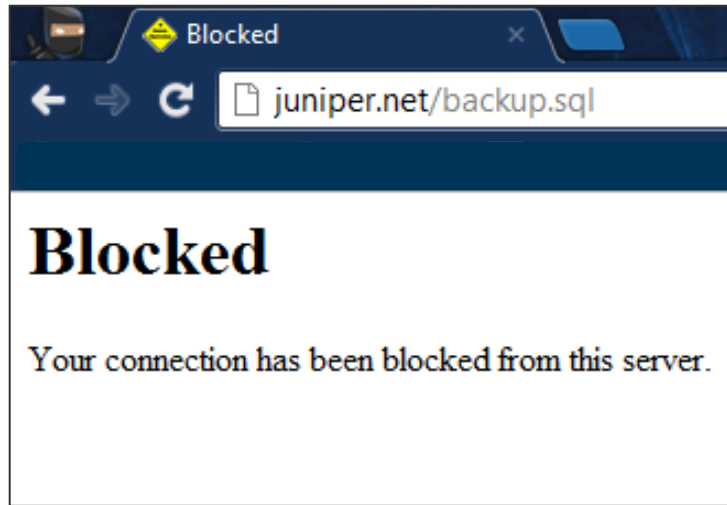
ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации



ОБНАРУЖЕНИЕ ЧЕРЕЗ ОБМАН ЗЛОУМЫШЛЕННИКА

Пример. Эмуляция уязвимого механизма аутентификации

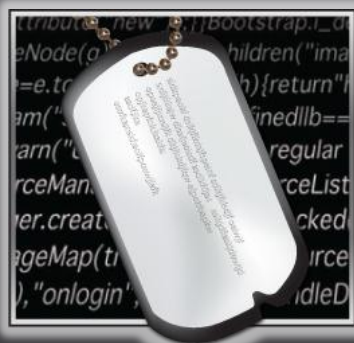


ОТСЛЕЖИВАНИЕ АТАКУЮЩЕГО НЕ ТОЛЬКО ЧЕРЕЗ IP-АДРЕС

Отслеживание IP адреса

Отслеживание браузера Цифровой токен

Во всех браузерах существует возможность сохранять различные контрольные данные



Отслеживание ПО, версии ОС и плагинов Отпечатки системы



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_АССЕРТ	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 сканирование	Сканирование 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

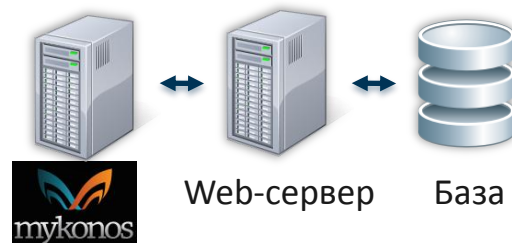
**РАЗВЕРТЫВАНИЕ
MYKONOS WEB SECURITY**

ТРИ ТИПА ВНЕДРЕНИЯ

ПО, устанавливаемое
на сервер или
виртуальная машина

Сервер MWS1000 с
преднастроенным ПО

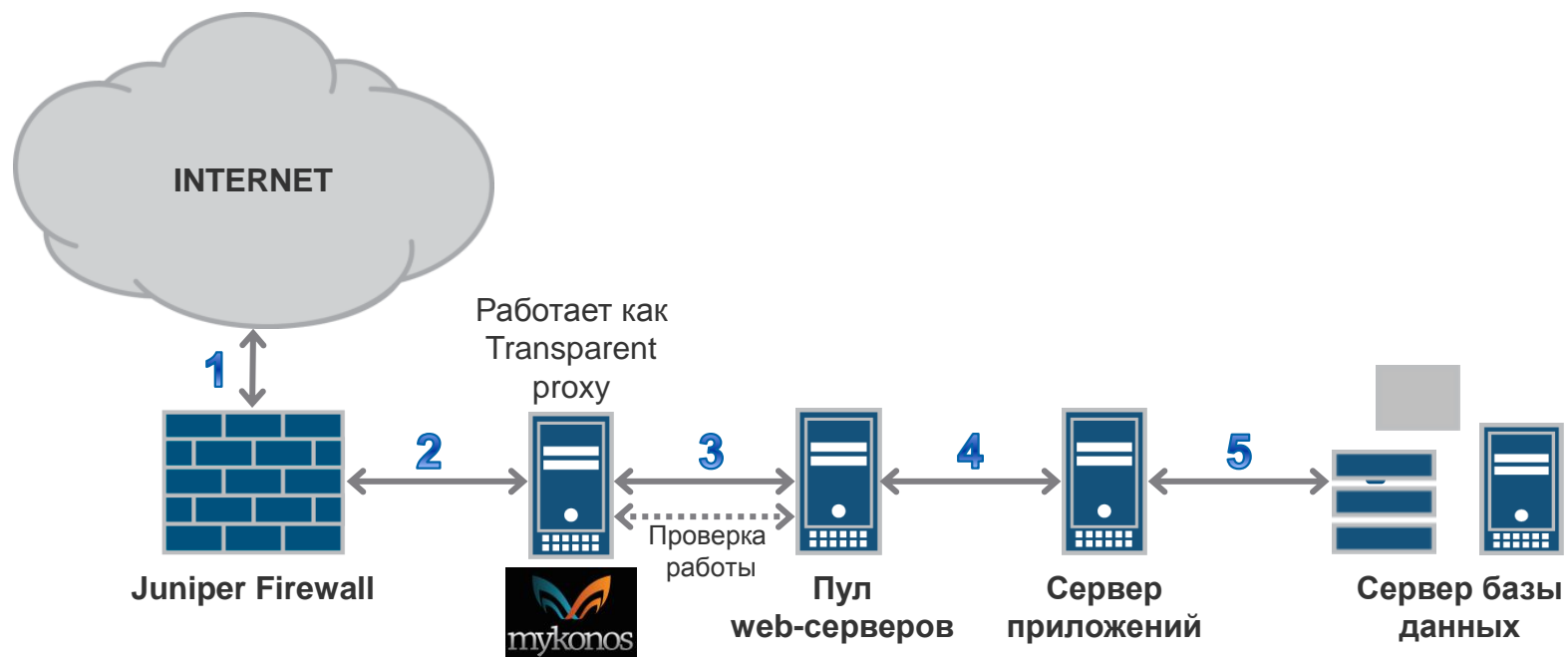
Для провайдеров
услуг web-хостинга



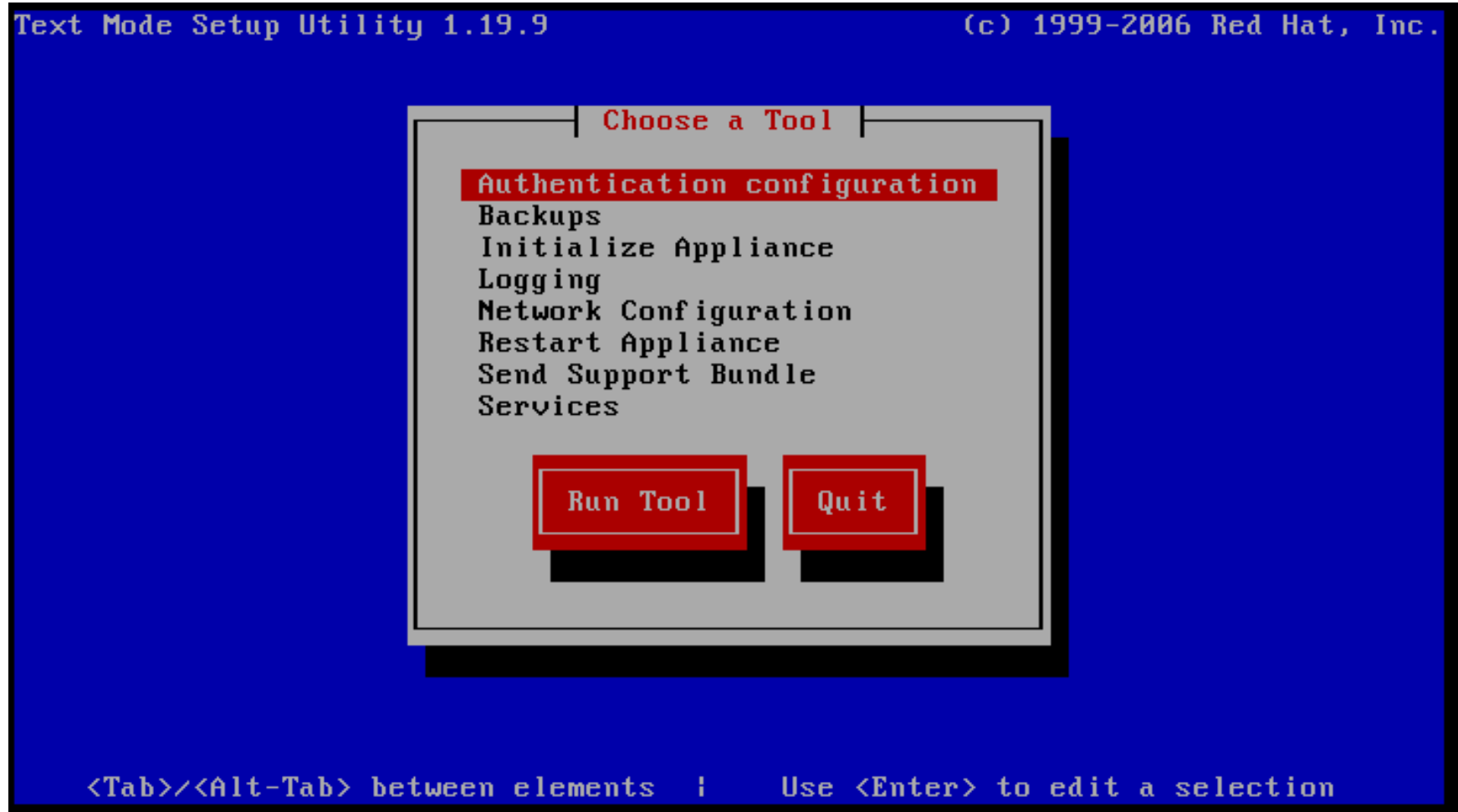
РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY РЕЖИМ REVERSE PROXY



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

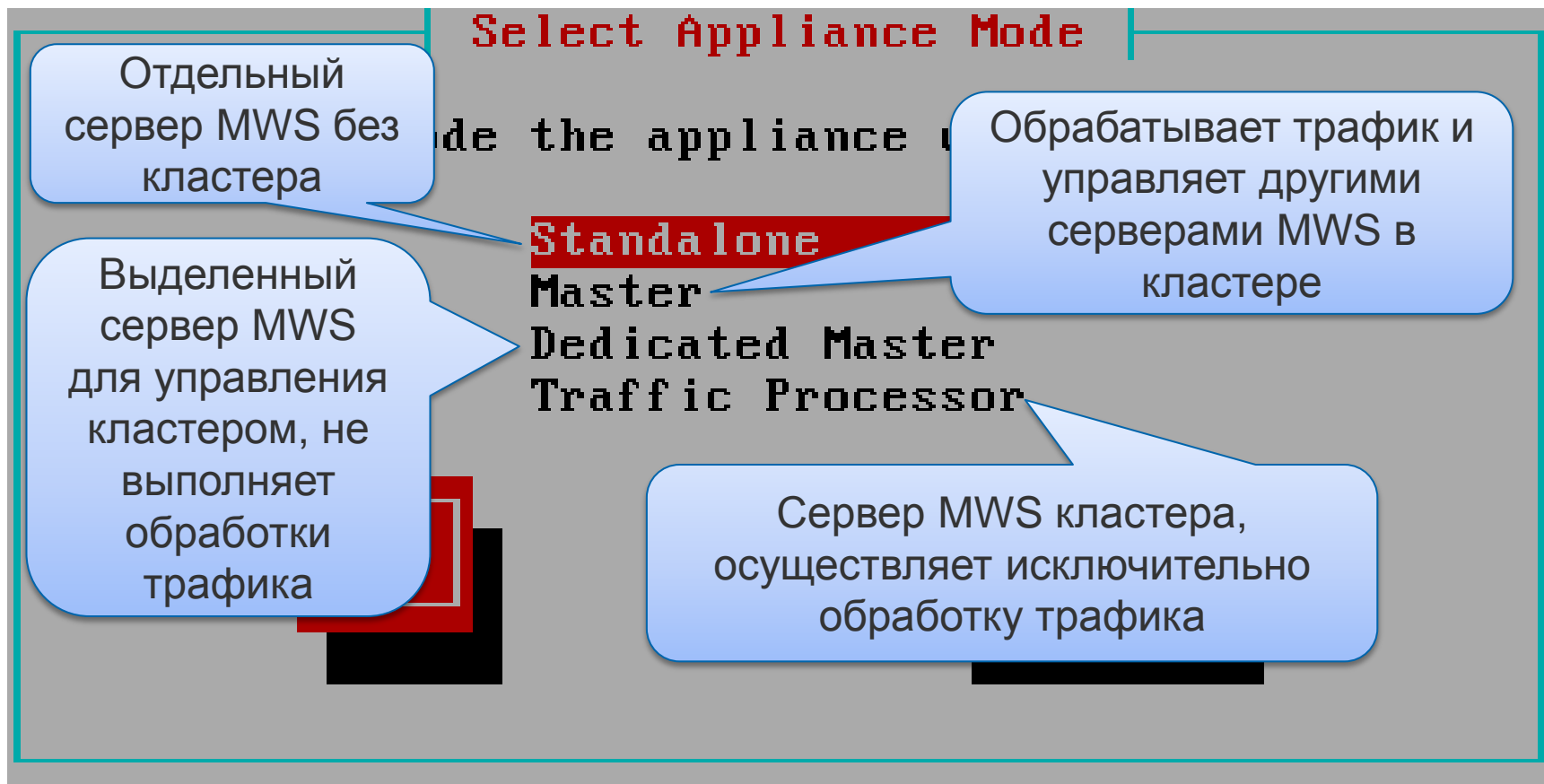
- Процессоры реагирования

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

**ΚΛΑΣΤΕΡ ΣΕΡΒΕΡΩΝ
ΜΥΚΟΝΟΣ WEB SECURITY**

РОЛИ СЕРВЕРОВ MWS В КЛАСТЕРЕ

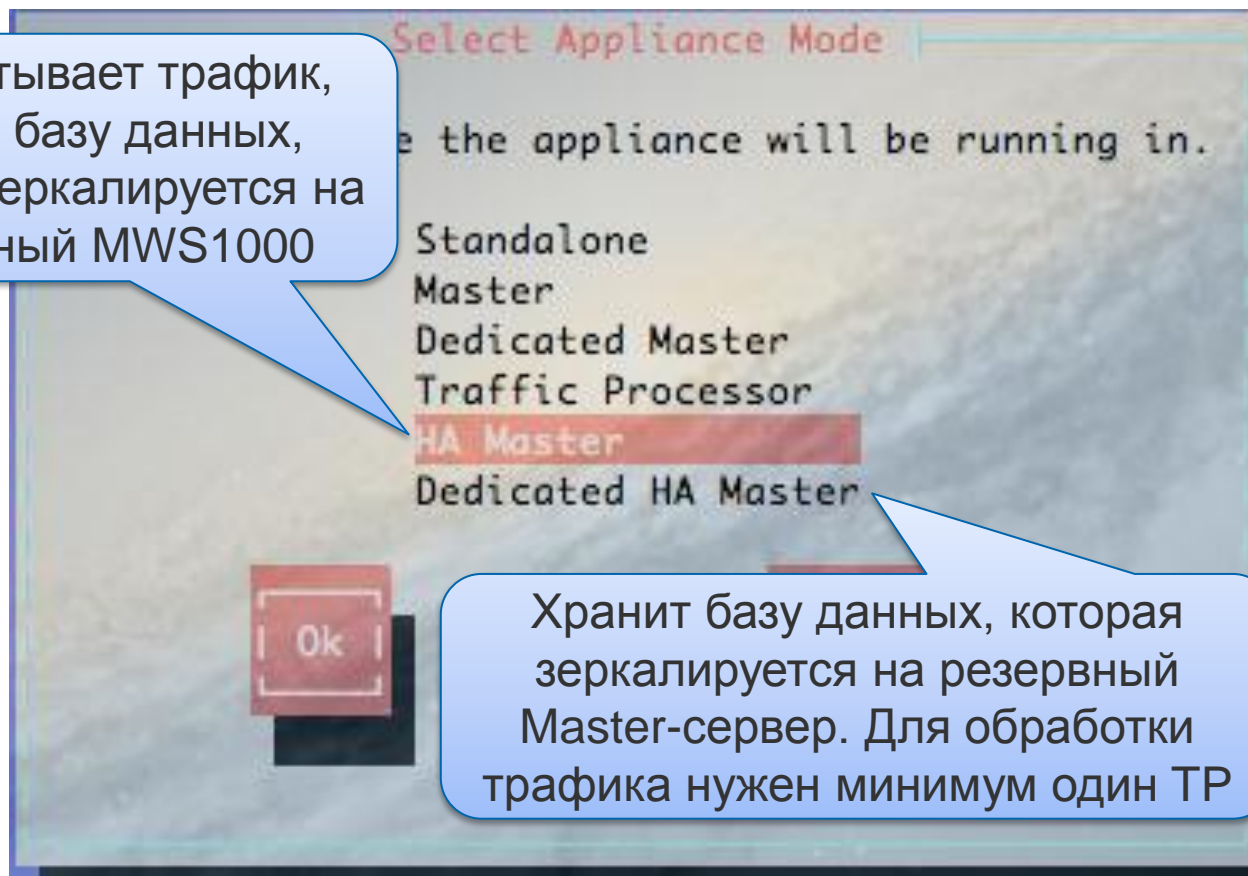


На Master и Dedicated Master располагается база данных, через них выполняется управление кластером

ОТКАЗОУСТОЙЧИВОСТЬ

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

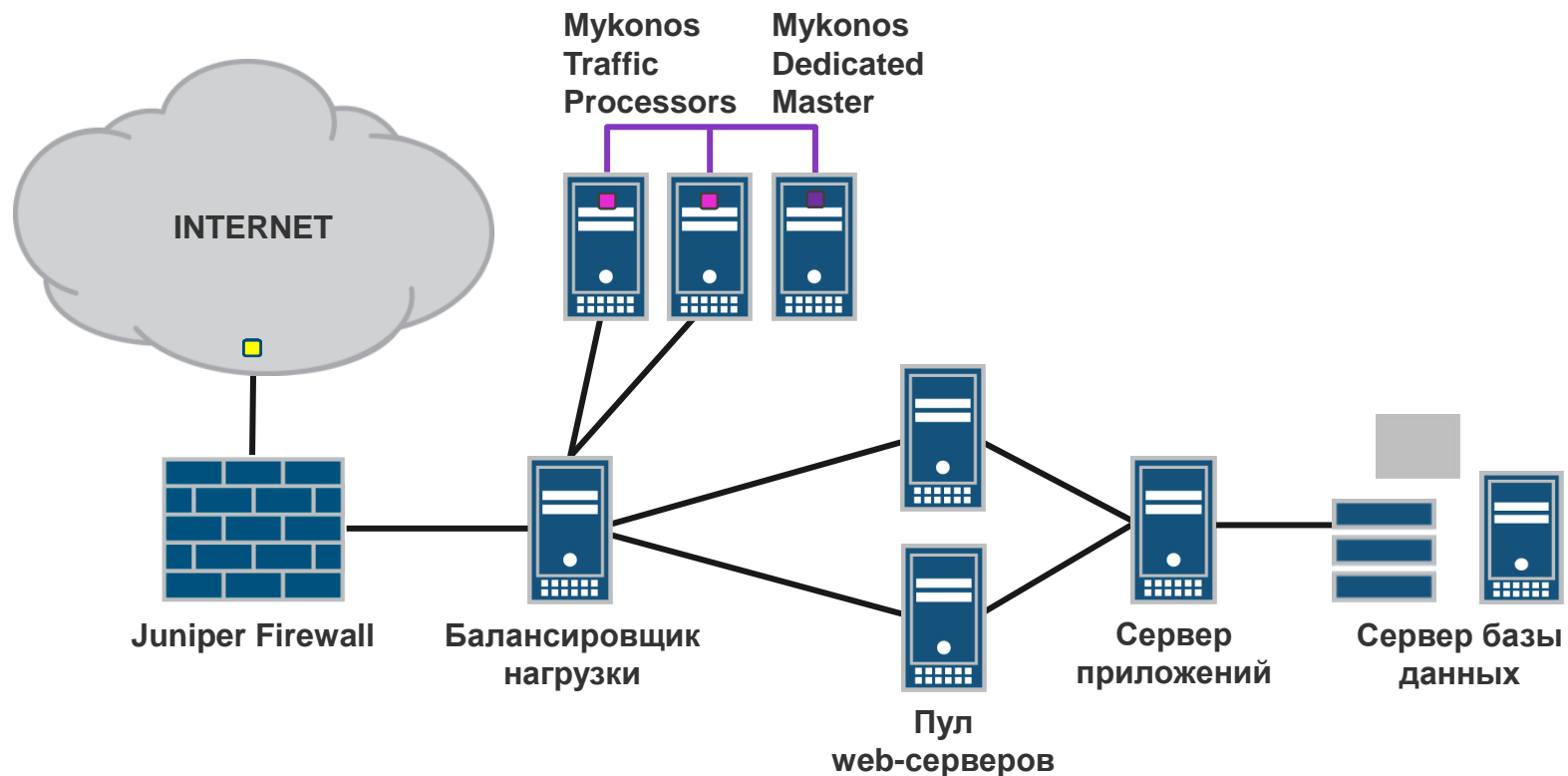
Обрабатывает трафик, хранит базу данных, которая зеркалируется на резервный MWS1000



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

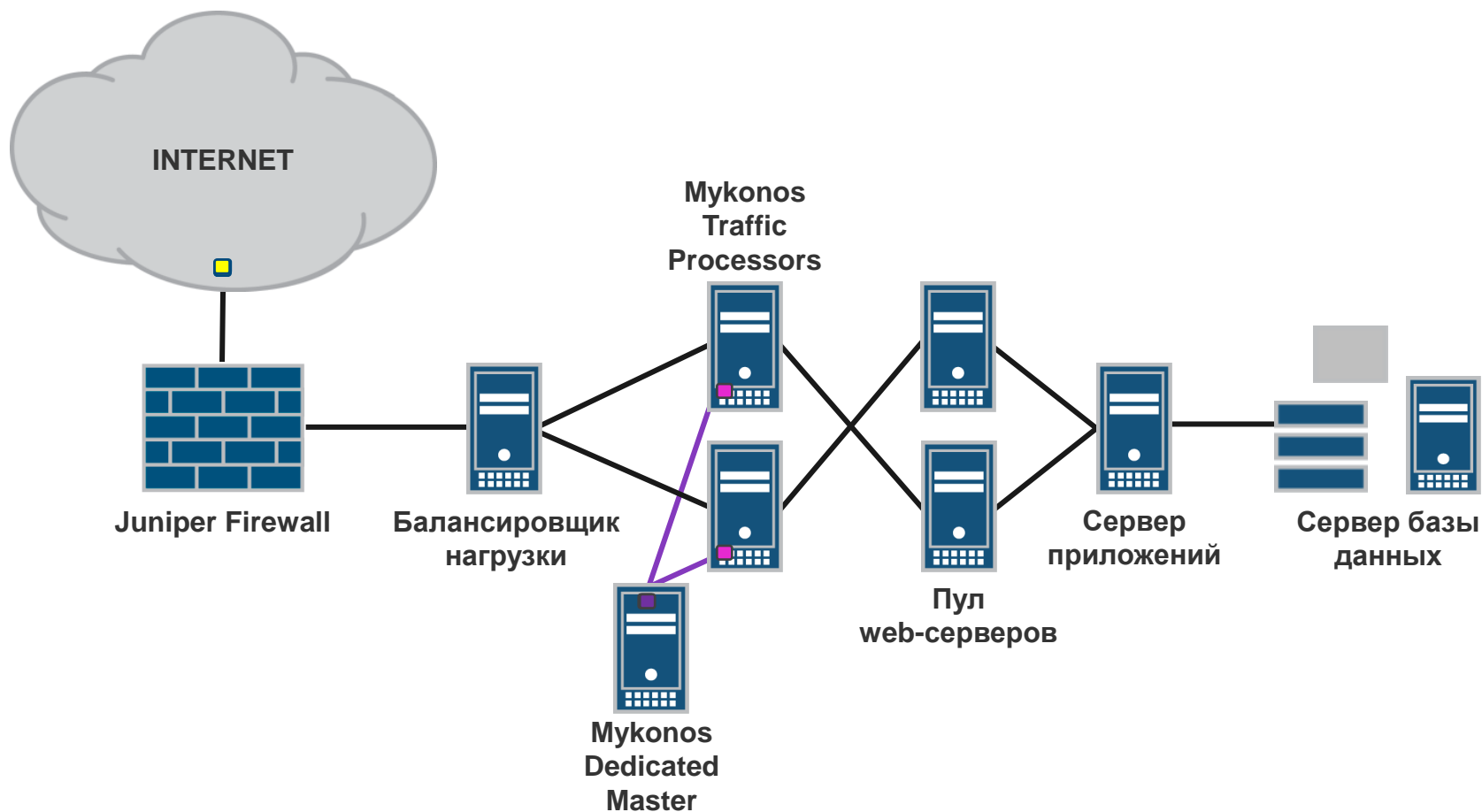
РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY

РАБОТА КЛАСТЕРА



РАЗВЕРТЫВАНИЕ MYKONOS WEB SECURITY





РАБОТА КЛАСТЕРА



**ИНТЕРФЕЙС
MYKONOS WEB SECURITY**

WEB-ИНТЕРФЕЙС НАСТРОЙКИ

The screenshot shows the Mykonos web interface. At the top left is the Mykonos logo. Below it is a navigation bar with buttons for Configuration, Autoresponses, Reports, System Status, Licensing, and Updates. On the left side, there is a sidebar menu with options: Basic Mode, Global Configuration, Services, Processors, Applications, Configuration Wizard, Expert Mode, and Import / Export. The main content area is titled "Configuration" and features four sections, each with an icon and a description:

- Basic Mode**:  Designed for technical and non-technical users alike, Basic Mode allows you to configure virtually every part of Mykonos Web Security.
- Configuration Wizard**:  Designed for a good "out-of-the-box" experience, the Configuration Wizard guides you, step-by-step, through the Mykonos Web Security configuration process.
- Expert Mode**:  Designed for seasoned users of Mykonos Web Security, the Expert Mode provides clean, no-frills access to every possible configuration parameter. **Unless you are ABSOLUTELY CERTAIN of what you are doing, we recommend using the Basic Mode or Configuration Wizard instead.**
- Import / Export**:  This option lets you import or export a complete "snapshot" of every configuration parameter available in Mykonos Web Security, and can aid with certain types of deployment.

Copyright © 2012 Mykonos Software. All Rights Reserved.
Third-Party License Information

WEB-ИНТЕРФЕЙС НАСТРОЙКИ ОСНОВНОЙ РЕЖИМ

Configuration » Basic Mode

Configuration: Basic Mode

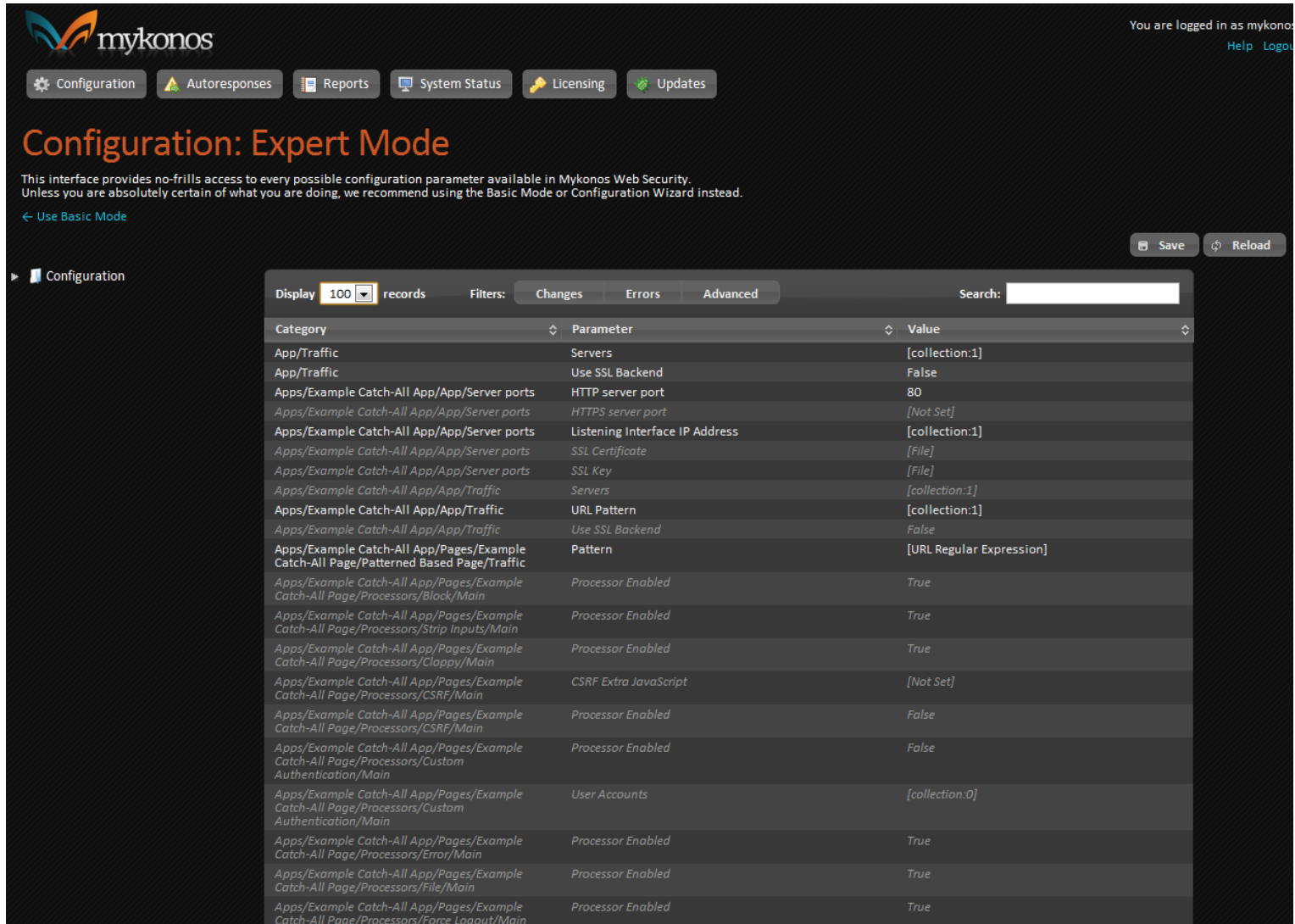
Global Configuration Services Processors Applications

Global

The global configuration defines the system's default actions, bindings, and preferences.

- » **Application — Identification**
The general configuration values for this application
- » **Application — Traffic**
The configuration information on how to identify this applications traffic
- » **Default Responses**
The default response definitions for any configured response that specifies that the default response for ...
- » **Error Handling**
Configuration for error handling and normalization
- » **General**
General configuration parameters
- » **General network settings**
Settings for general networking
- » **Incident Monitoring**
The collection of incidents to monitor
- » **Logging**
Logging configuration
- » **SMTP**
Configuration for messaging
- » **Security**
The global security configuration
- » **Security Monitor**
Security monitor configuration
- » **Server ports**
Server port configuration
- » **Session Management**
Configuration for session management

WEB-ИНТЕРФЕЙС НАСТРОЙКИ ЭКСПЕРТНЫЙ РЕЖИМ



mykonos

You are logged in as mykonos
[Help](#) [Logout](#)

Configuration Autoresponses Reports System Status Licensing Updates

Configuration: Expert Mode

This interface provides no-frills access to every possible configuration parameter available in Mykonos Web Security. Unless you are absolutely certain of what you are doing, we recommend using the Basic Mode or Configuration Wizard instead.

[← Use Basic Mode](#)

Save Reload

Configuration

Display 100 records Filters: Changes Errors Advanced Search:

Category	Parameter	Value
App/Traffic	Servers	[collection:1]
App/Traffic	Use SSL Backend	False
Apps/Example Catch-All App/App/Server ports	HTTP server port	80
Apps/Example Catch-All App/App/Server ports	HTTPS server port	[Not Set]
Apps/Example Catch-All App/App/Server ports	Listening Interface IP Address	[collection:1]
Apps/Example Catch-All App/App/Server ports	SSL Certificate	[File]
Apps/Example Catch-All App/App/Server ports	SSL Key	[File]
Apps/Example Catch-All App/App/Traffic	Servers	[collection:1]
Apps/Example Catch-All App/App/Traffic	URL Pattern	[collection:1]
Apps/Example Catch-All App/App/Traffic	Use SSL Backend	False
Apps/Example Catch-All App/Pages/Example Catch-All Page/Patterned Based Page/Traffic	Pattern	[URL Regular Expression]
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Block/Main	Processor Enabled	True
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Strip Inputs/Main	Processor Enabled	True
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Cloppy/Main	Processor Enabled	True
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/CSRF/Main	CSRF Extra JavaScript	[Not Set]
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/CSRF/Main	Processor Enabled	False
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Custom Authentication/Main	Processor Enabled	False
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Custom Authentication/Main	User Accounts	[collection:0]
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Error/Main	Processor Enabled	True
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/File/Main	Processor Enabled	True
Apps/Example Catch-All App/Pages/Example Catch-All Page/Processors/Force Logout/Main	Processor Enabled	True

WEB-ИНТЕРФЕЙС МОНИТОРА БЕЗОПАСНОСТИ



ПОДРОБНЫЙ ПРОФИЛЬ АТАКУЮЩЕГО

Каждому атакующему назначается имя

The screenshot displays a security dashboard for an attacker named 'Jack 26'. The interface includes a profile card on the left with a gear icon and a 'Threat: Extreme' label. A central table lists various incidents, with 'Password Cracked' highlighted in orange. A callout box labeled 'История инцидента' points to this row. The table has columns for incident names and complexity levels.

Incidents	Complexity
Hidden Parameter Manipulation	Medium
Illegal Response Status	High
Password Cracked	Extreme
Protected Resource Requested	High
Apache Password File Requested	Medium
Apache Configuration Requested	Medium
Hidden Parameter Manipulation	Medium
Query Parameter Manipulation	Low

Опасность атакующего

ПРИМЕР. ОТСЛЕЖИВАНИЕ ЗЛОУМЫШЛЕННИКА

Sessions

Remote Address	Browser	Operating System	Location	Requests	Errors	Profile Name
203.187.204.245	Chrome 21.0.1180.79	Windows 7	IN - Gujarat	9	0	Lula 9019
121.31.182.217	Chrome 21.0.1180.79	Windows 7	CN - Guangxi	190	1	Rosalinda 3374
121.31.182.217	Chrome 21.0.1180.79	Windows 7	CN - Guangxi	8	0	Lottie 4004
121.33.239.142	Unknown Unknown	Unknown	CN - Guangdong	1	0	Carlos 5723
221.128.114.115	Unknown Unknown	Unknown	TH - Unknown	1	0	Vilma 1639
66.108.5.107	Internet Explorer 6.0	Windows XP	US - New York	1	1	
75.138.178.141	Unknown Unknown	Unknown	US - Massachusetts	421	237	Maura 3108
75.138.178.141	Internet Explorer 9.0	Windows 7	US - Massachusetts	10	0	
75.138.178.141	FireFox 14.0.1	Macintosh OS	US - Massachusetts	219	3	Cristina 258
75.138.178.141	Unknown Unknown	Unknown	US - Massachusetts	9	0	
75.138.178.141	Unknown Unknown	Unknown	US - Massachusetts	77	56	Deanne 7575
75.138.178.141	Unknown Unknown	Unknown	US - Massachusetts	3	3	

8 minutes ago

Session

121.31.182.217

Nanning Guangxi, Rosalinda 3374

Requests: 190
Errors: 1

Last Active: 8 minutes ago
First Active: 1 hour ago

Incidents	Locations	Environments
Direct	Remote Address: 212.44.135.114, Host: 212, City: Smolenskaya, Region: Krasnodar	Postal Code: , Country: Russian Federatio, Requests: 165, Errors: 1
Direct	Remote Address: 121.31.182.217, Host: 121, City: Nanning, Region: Guangxi	Postal Code: , Country: China, Requests: 18, Errors: 0
Direct	Remote Address: 164.77.196.78, Host: 164, City: Santiago, Region: Region Metropolitana	Postal Code: , Country: Chile, Requests: 7, Errors: 0
Direct	Remote Address: 58.248.217.209, Host: 58.2, City: Guangzhou, Region: Guangdong	Postal Code: , Country: China, Requests: 11, Errors: 0
Direct	Remote Address: 50.22.206.184, Host: 50.2, City: Dallas, Region: Texas	Postal Code: 75207, Country: United States, Requests: 5, Errors: 0

First Active: 1 hour ago, Last Active: 8 minutes ago

First Active: 20 minutes ago, Last Active: 15 minutes ago

First Active: 31 minutes ago, Last Active: 30 minutes ago

First Active: 32 minutes ago, Last Active: 31 minutes ago

First Active: 34 minutes ago, Last Active: 34 minutes ago

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 проху

Позволяет проанализировать когда с какого адреса работал атакующий

ДААННЫЕ ПО ИНЦИДЕНТУ

Выбор инцидента


Security Monitor 4.2.0-2

Incidents last 7 days ▼

Incident Name	Profile	Complexity	Count	First Time	Last Time
Password Cracked	Joanne 3813	High	1	13 hours ago	13 hours ago
Protected Resource Requested	Joanne 3813	Low	1	13 hours ago	13 hours ago
Apache Password File Requested	Joanne 3813	Low	1	13 hours ago	13 hours ago
Apache Configuration Requested	Joanne 3813	Low	1	13 hours ago	13 hours ago
Hidden Parameter Manipulation	Joanne 3813	Medium	1	13 hours ago	13 hours ago
Query Parameter Manipulation	Joanne 3813	Low	9	13 hours ago	13 hours ago
Query Parameter Manipulation	Shane 8545	Low	1	08/16/2012 03:48:36	08/16/2012 03:48:36
Password Cracked	Lorena 5622	High	1	08/16/2012 00:50:50	08/16/2012 00:50:50
Apache Password File Requested	Lorena 5622	Low	1	08/16/2012 00:49:34	08/16/2012 00:49:34
Apache Configuration Requested	Lorena 5622	Low	1	08/16/2012 00:49:13	08/16/2012 00:49:13
Hidden Parameter Manipulation	Lorena 5622	Medium	2	08/16/2012 00:32:22	08/16/2012 00:32:37
Query Parameter Manipulation	Lorena 5622	Low	3	08/16/2012 00:29:27	08/16/2012 00:30:48
Common Directory Enumeration	Jan 3572	Medium	3	08/14/2012 16:50:30	08/15/2012 16:50:35

Search Clear Search 1 of 3

Incident: Password Cracked 13 hours ago


Password Cracked (High)

Joanne 3813
Sunnyvale California, United States
FireFox 14.0.1 (Windows 7)
Session

Last Time: 13 hours ago
First Time: 13 hours ago

Description		Details	
Name	Value		
username	Barton		
password	trapper		
url	http://demo.mykonossoftware.com:80/backup.sql		
referer	http://demo.mykonossoftware.com/backup.sql		
incidentCount	1		

Request Response

Детали инцидента

ПРИМЕРЫ ОТЧЕТОВ

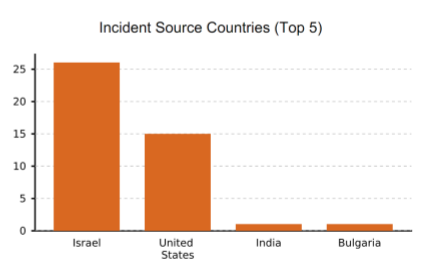
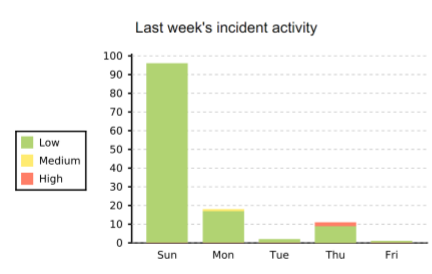
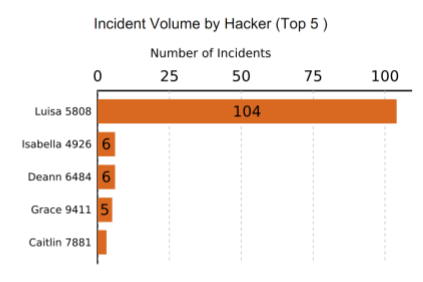
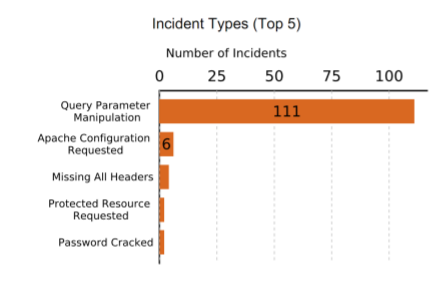
Created	User Agent	Request Content	Response Content
03-Aug-12 11:11	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)	POST /?action=cart HTTP/1.1 host: demo.mykonossoftware.com x-forwarded-for: 66.129.224.36 x-myk-request-info: http, HTTP/1.1, 80 x-myk-appid: 171544 x-myk-port: 80 x-myk-use-ssl: false x-myk-ssl: 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=tlu96qgZhuqghup6mfm0; PHPSESSID_s=0438cd92a223e3a96db30745ae6bca content-type: application/x-www-form-urlencoded content-length: 28 x-myk-access-log-id: CE2C895E-97C0-4A89-8CE9-82907ED1A613 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 XHTML//EN//EN"> <html> <head> <title>Generic Electronics</title> <meta http-equiv="content-type" content="text/html; charset=UTF-8" /> <link rel="stylesheet" href="/css/style.css" type="text/css" /> <link rel="stylesheet" href="/css/print.css" type="text/css" /> <script type="text/javascript" src="/js/jquery.js" /> <script type="text/javascript" src="/js/jquery.cookie.js" /> <script type="text/javascript" src="/js/jquery.validate.js" /> <script type="text/javascript" src="/js/jquery.form.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> </script> </head> <body> <div class="main">
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=tlu96qgZhuqghup6mfm0; PHPSESSID_s=0438cd92a223e3a96db30745ae6bca 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 XHTML//EN//EN"> <html> <head> <title>Generic Electronics</title> <meta http-equiv="content-type" content="text/html; charset=UTF-8" /> <link rel="stylesheet" href="/css/style.css" type="text/css" /> <link rel="stylesheet" href="/css/print.css" type="text/css" /> <script type="text/javascript" src="/js/jquery.js" /> <script type="text/javascript" src="/js/jquery.cookie.js" /> <script type="text/javascript" src="/js/jquery.validate.js" /> <script type="text/javascript" src="/js/jquery.form.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> <script type="text/javascript" src="/js/jquery.easing.js" /> <script type="text/javascript" src="/js/jquery.scrollTo.js" /> </script> </head> <body> <div class="main">

Детализация инцидентов по IP-адресу

Обобщенные данные

Hacker Detection & Prevention Scorecard Mykonos System Report <http://www.mykonossoftware.com/>

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



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 SVC-COR-MWS100MB	Поддержка MWS1000	---
	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