

ALL-IN-ONE: КАК СДЕЛАТЬ ПРОЕКТ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ

Дмитрий Борисов

Инженер-проектировщик по ИБ
dp.borisov@jet.su

ЗАКАЗЧИК И ОТНОШЕНИЯ С ДЖЕТ



- Один из крупных региональных банков (ТОП-50)
- Почти **4000** сотрудников,
более **700 000** клиентов-физических лиц
и **15 000** корпоративных клиентов
- Более **10** совместных проектов:
 - Внедрение HP Arcsight (2014 г.)
 - Внедрение McAfee Web | Mail Gateway и McAfee Network DLP (2014 г.)
 - Внедрение Imperva DAM (2015 г.) и модернизация (2017 г.)
 - Аудиты на соответствие PCI DSS (2014 - 2017 г.)



НА ИСХОДНУЮ!



- **Цели Заказчика**

- обновление текущих решений по ИБ
- возможность администрирования малыми ресурсами
- противодействие целенаправленным атакам и «zero-day»-угрозам

- **Три гео-распределенные площадки:**

- Центральный офис/ЦОД
- Резервный ЦОД
- Процессинговый центр



У ВАС ЕСТЬ ПРОБЛЕМА? У НАС ЕСТЬ РЕШЕНИЕ



ЦЕНТРАЛЬНЫЙ ОФИС/ЦОД

РЕЗЕРВНЫЙ ЦОД

ПРОЦЕССИНГОВЫЙ ЦЕНТР



МОНОВЕНДОРНОСТЬ ХОРОШО ИЛИ ПЛОХО?



FORTINET®



КОНФИДЕНТ®
CONFIDENT

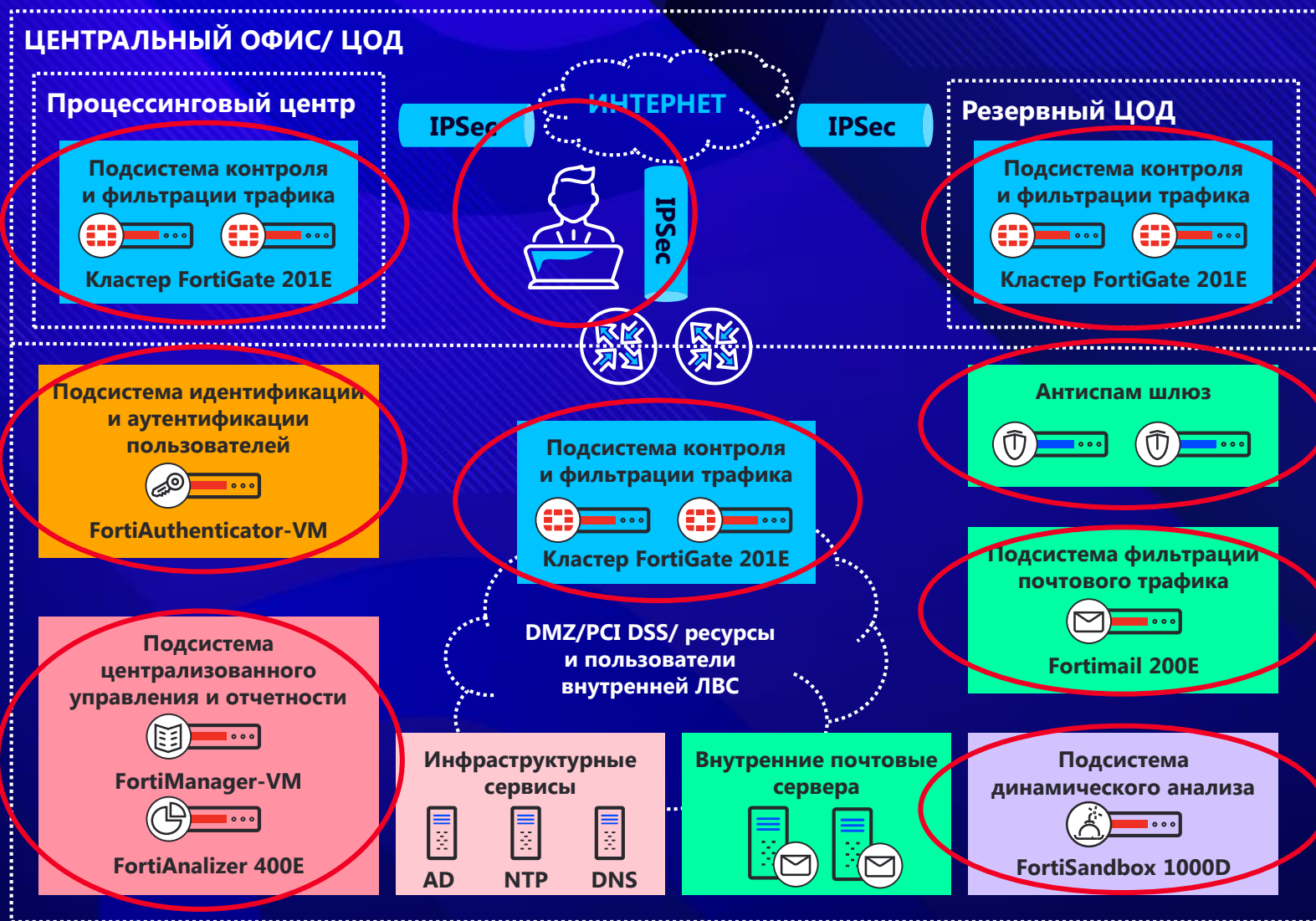


КОД БЕЗОПАСНОСТИ

АПР [★]ОКБ

s•terra

#АРХИТЕКТУРА ПРОЕКТА



ОСТАВИМ ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ — У НАС ЖЕ СТЕНД-АП!



ОБЛАЧНЫЕ ТЕХНОЛОГИИ В ДЕЙСТВИИ



ИНСТРУМЕНТОВ, КОТОРЫЕ ПОЯВИЛИСЬ У ЗАКАЗЧИКА

5 МЕСТО

ВСТРОЕННЫЙ АУДИТ НА СООТВЕТСТВИЕ PCI DSS

★ Favorites	#	Date/Time	Level	Message	Result
Dashboard	24	2 minutes ago		Check that the hit count is enabled for FGT	✓
Security Fabric	25	2 minutes ago		Check that Out of State TCP Packets are dropped	✓
FortiView	26	2 minutes ago		Check the ICMP Virtual Session Timeout is set	✗
Network	27	2 minutes ago		Check the UDP Virtual Session Timeout is set	✗
System	28	2 minutes ago		Check the TCP End Timeout is set	✓
Policy & Objects	29	2 minutes ago		Check the TCP Session Timeout is set	✓
Security Profiles	30	2 minutes ago		Check TCP start timeout is set	✓
VPN	31	2 minutes ago		Check session start log enabled with log all traffic configured	✗
User & Device	32	2 minutes ago		Check invalid packets are logged	✗
Log & Report	33	2 minutes ago		Check that system administrator activities are logged	✓
Forward Traffic	34	2 minutes ago		Check that NAT/PAT is enabled in the Firewall settings	✓
Local Traffic	35	2 minutes ago		Check that Firewall logs are only deleted when available disk space reaches a minimum level	✓
Sniffer Traffic	36	2 minutes ago		Check that an available disk space low alert event is logged	✓
System Events	37	2 minutes ago		Check the minimum threshold 70 percent set for the available disk space alert for the logs	✗
Router Events	38	2 minutes ago		Check that there are alerts to monitor the available disk space for the Firewall logs	✓
VPN Events	39	2 minutes ago		Check Firewall logs are being saved on a remote log server	✓
User Events	40	2 minutes ago		Check 'Implicit Deny Rule' is defined in Firewall Rule Base	✓
Endpoint Events	41	2 minutes ago		Check SSH-SSL deep inspection enabled on FGT with App Control enabled	✗
HA Events	42	2 minutes ago		Check the SSH-SSL deep inspection with the App Control enabled drops traffic from servers with invalide certificate	✗
WAN Opt. & Cache Events	43	2 minutes ago		Check daily scheduled update enabled for the Application database	✓
Compliance Events	44	2 minutes ago		Check the Application Database auto-update enabled	✓
AntiVirus	45	2 minutes ago		Check App Control policy blocks proxy applications	✗
	46	2 minutes ago		Check App Control policy blocks P2P applications	✗
	47	2 minutes ago		Check App Control policy blocks File storage applications	✗
	48	2 minutes ago		Check AV scan is activated according to the policy	✗
	49	2 minutes ago		Check daily scheduled update enabled for the AV database	✓
	50	2 minutes ago		Check the AV signature database auto-update enabled	✓

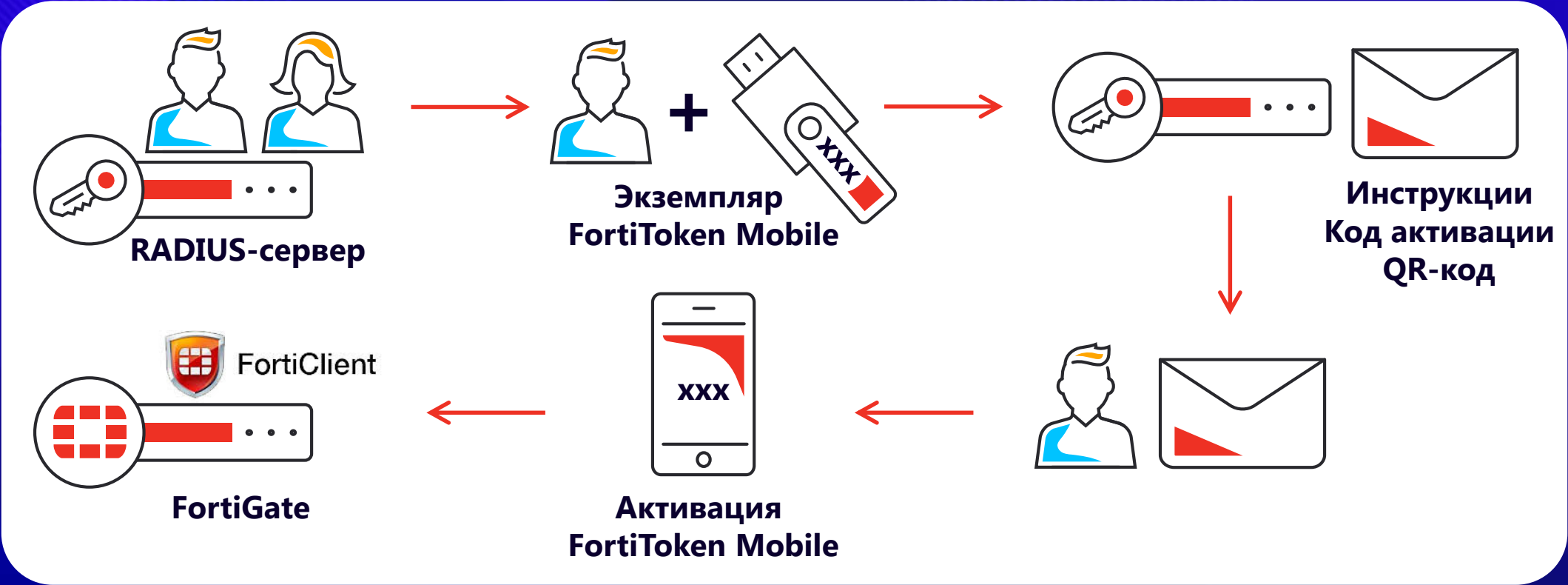
4 МЕСТО

УПРАВЛЕНИЕ ВСЕМ ИЗ ОДНОЙ КОНСОЛИ



3 МЕСТО

2FA ПРИ УДАЛЕННОМ ДОСТУПЕ



2 МЕСТО

А ДЛЯ ТЕХ КТО ЛЮБИТ ОЛДСКУЛ И ПРЕДАННЫХ ФАНАТОВ ЗМЕЙКИ...ПРИХОДЯТ СМС



1 МЕСТО

ГДЕ АТАКА? ВОТ ЖЕ ОНА...

High Risk Downloader

Mark as clean (false positive)

Received	Apr 25 2018 06:00:26
Started	Apr 25 2018 06:00:28
Status	Done
Rated By	VM Engine
Submit Type	FortiMail
Source IP	[REDACTED]
Destination IP	[REDACTED]
Digital Signature	No
Virus Total	Q

ВЕРДИКТ ВЫДАЛА VM

More Details

Packers	Microsoft Visual C++ v8.0
File Type	exe
Downloaded From	3859217543183212075~
File Size	479232 (bytes)
Email Sender	fjuhvi1952@yahoo.co.uk
Email Receiver	[REDACTED]
MD5	9ed70f5f2674f7143d8033c7f8216216
SHA1	4ece73cc7495051eccdffe377817875a67fcd895
SHA256	1a801e0b693052cc97e63eac94d8a4a0efa5ae1df98053f7b89be15d290bbf68
ID	3859217565276787842
Submitted By	[REDACTED]
Submit Device	[REDACTED]
DOMAIN/VDOM	[REDACTED]
Submitted Filename	w3P61n2f020438-w3P61n2h020438.2018-04-25.09:01:50.3#рекламзиты.scr.gz
Filename	3859217543183212075~
Start Time	Apr 25 2018 06:00:28
Detection Time	Apr 25 2018 06:02:48
Scan Time	140 seconds
Scan Unit	[REDACTED]
Device	[REDACTED]
Launched OS	WIN7X64VM
Infected OS	WIN7X64VM

Analysis Details

WIN7X64VM

[Captured Packets](#)
[Original File](#)
[Tracer Package](#)
[Tracer Log](#)

Behavior Chronology Chart

Threat Level vs Time

● Low Risk ● Clean

Suspicious Indicators (4)

- Virus detected
- Suspicious IP
- This file checked registry for anti-virtualization or anti-debug
- Suspicious registry

Static Analysis (1)

- Files Created (2)
- Launched Processes (3)
- Registry Changes (2)
- Network Behaviors (74)
- Behaviors In Sequence (165)

Tracer Package Version: 02005.00518 Rating Package Version: 02005.00518

ИНДИКАТОРЫ УГРОЗЫ СИГНАТУРНЫЙ АНАЛИЗ ЗДЕСЬ БЕСПОМОЩЕН

ПОДВОДИМ ИТОГИ



- **В НОГУ СО ВРЕМЕНЕМ**

ПОЛНОЦЕННЫЕ NGFW С SSL-ИНСПЕКЦИЕЙ,
КОНТРОЛЕМ ПРИЛОЖЕНИЙ И МНОГИМ ДРУГИМ

- **С РАСЧЕТОМ НА БУДУЩЕЕ**

ЕОЛ ТЕПЕРЬ НЕ СТРАШЕН

- **БЕЗОПАСНЕЕ**

ЗАЩИТА ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК И 2FA



СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Борисов

Инженер-проектировщик по ИБ
dp.borisov@jet.su

