ITSF

XIII ЦИФРОВОЙ ФОРУМ

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ РЕШЕНИЙ NGFW

Михаил Черкашин

Очень частая ситуация

Под проект был куплен межсетевой экран 

Его настройка выполнялась только на старте проекта 

Сопровождение сводится к созданию новых правил 

Текущий результат …. 

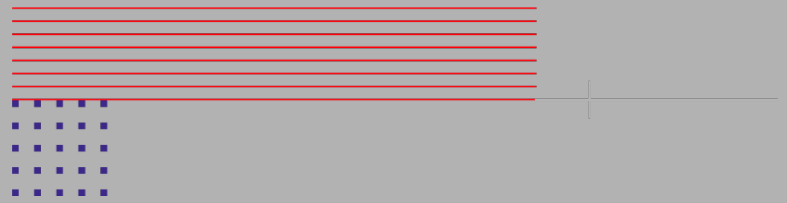
Что мы рассмотрим

Зачем производить оптимизацию

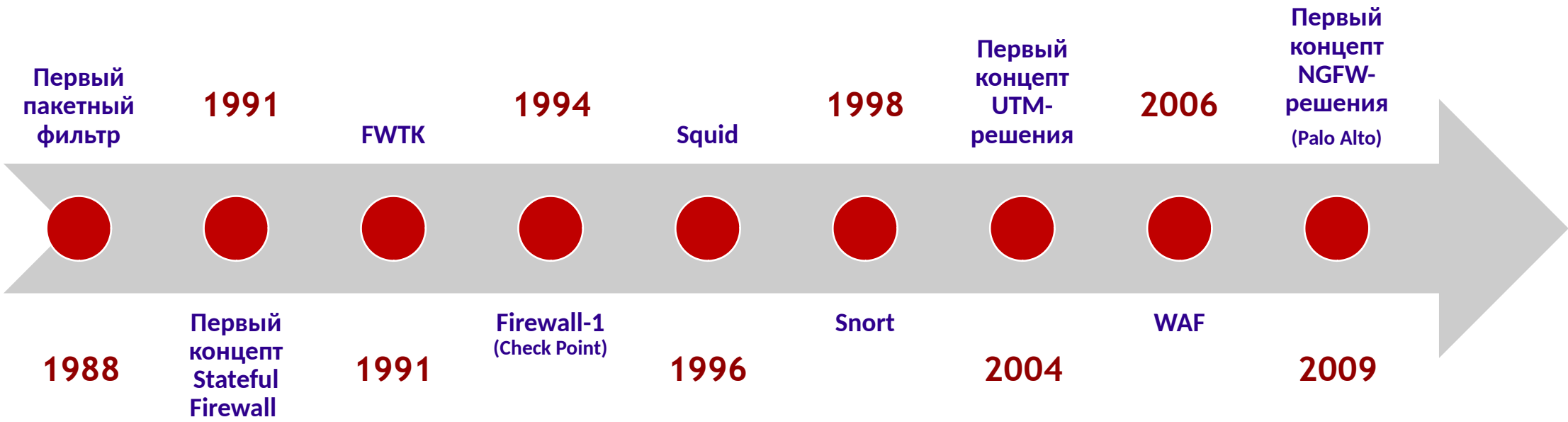
Что мы можем и не можем оптимизировать

Как это всё отслеживать...

Зачем нужно что-то оптимизировать?



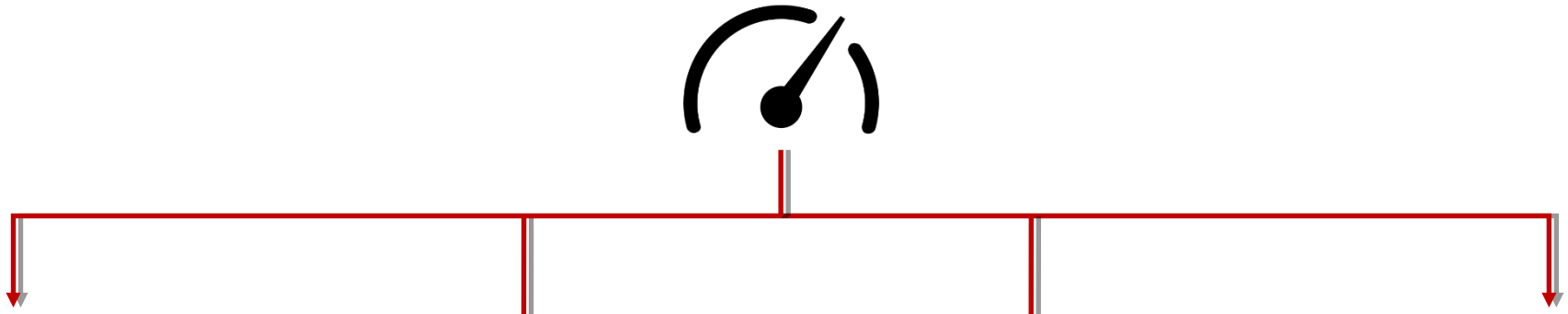
Эволюция межсетевого экрана



Что можно сделать?

- ✓ **Уменьшить** количество **сбоев** защищаемых сервисов
- ✓ **Увеличить производительность** NGFW путем оптимизации настроек
- ✓ **Выявлять** потенциальные **проблемы** ещё до их появления

Виды оптимизации производительности NGFW

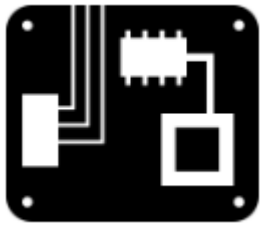


Оптимизация параметров конфигурации

Оптимизация кода продукта

Долго и сложно

Замена «железа»



Дорого

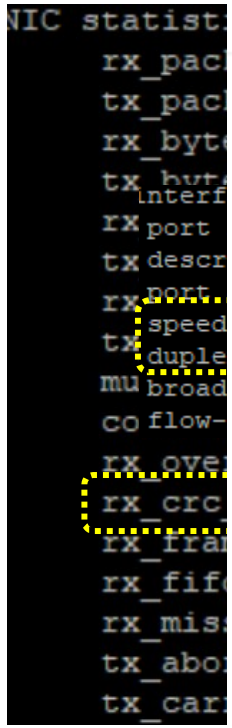
Оптимизация политик фильтрации

Оптимизация NGFW Check Point

Ускорение обработки трафика

- Проверьте настройки сетевых интерфейсов (**скорость, RX-ERR, RX-OVR, RX-DRP, очереди обработки**)
- Используйте Gaia 64-bit mode (**нужно 6Gb RAM на шлюзе**)
- Проверьте использование CoreXL (**SND/IRQ**) и SecureXL (**F2F, PXL, SXL**)
- Используйте современные протоколы шифрования (**AES**)

Ошибки в защищаемых сервисах из-за ошибок конфигурирования (L1-L3)



Symptoms

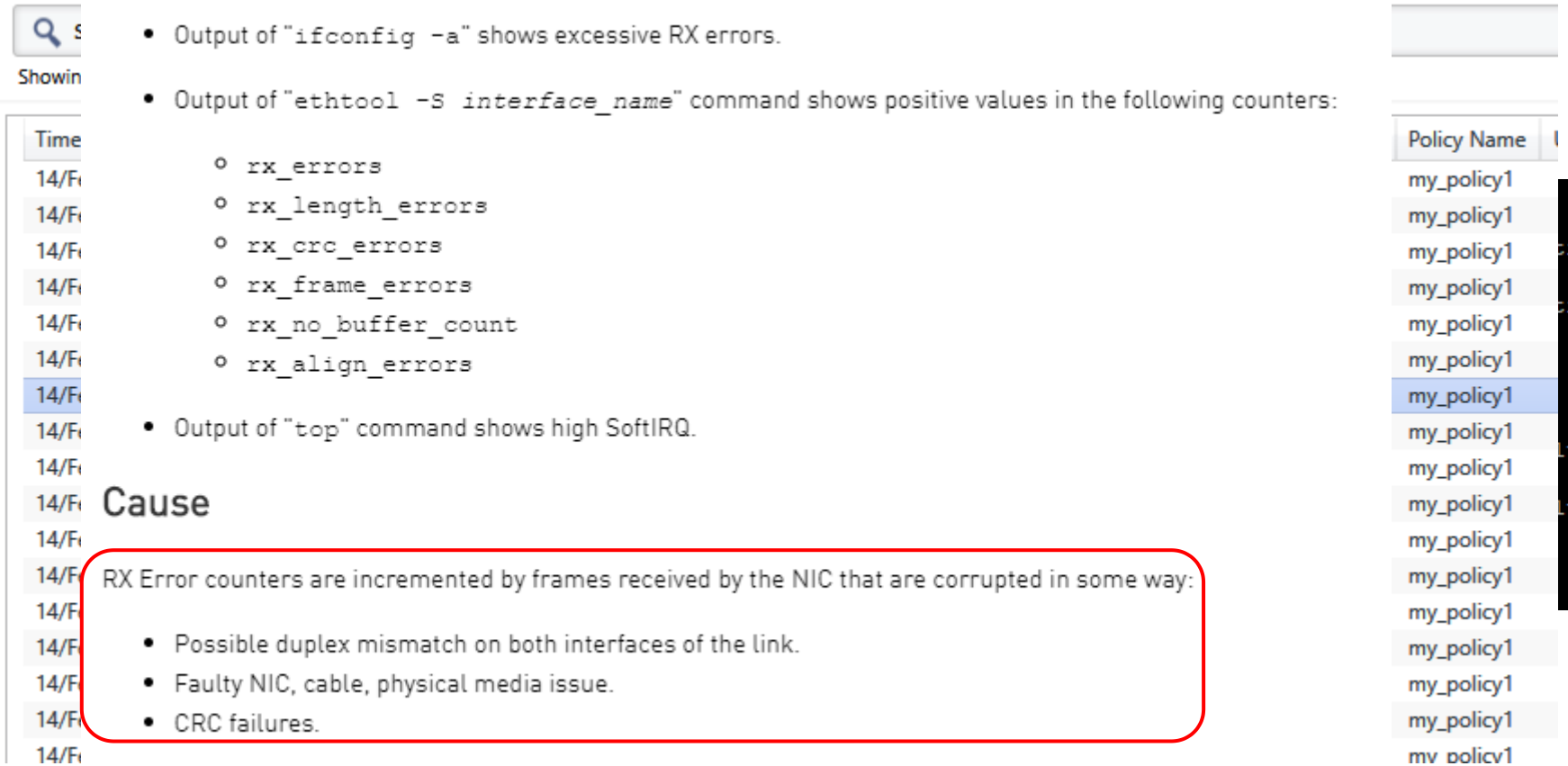
- Output of "`ifconfig -a`" shows excessive RX errors.
- Output of "`ethtool -S interface_name`" command shows positive values in the following counters:
  - `rx_errors`
  - `rx_length_errors`
  - `rx_crc_errors`
  - `rx_frame_errors`
  - `rx_no_buffer_count`
  - `rx_align_errors`
- Output of "`top`" command shows high SoftIRQ.

Cause

RX Error counters are incremented by frames received by the NIC that are corrupted in some way:

- Possible duplex mismatch on both interfaces of the link.
- Faulty NIC, cable, physical media issue.
- CRC failures.

In addition, NIC speed / duplex mis-match with the connecting port on the switch/router might be the cause.



Счетчики ERR, DRP, OVR

```
[Expert@firewall:0]# netstat -ni
Kernel Interface table
Iface  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR
eth0  799796      1      0      0   917594      0      0      0
eth1  521824      2      4      0  1342053      0      0      0
eth2  467258      0      0      0   459184      0      0      0
eth3  467032      0      0      0  5944661      0      0      0
lo    285998      0      0      0   285998      0      0      0
[Expert@firewall:0]#
```

tcpdump –c 100 -eni eth0 not ether proto 0x0800 and not ether proto 0x0806

(IPv4) (ARP)

tcpdump –c 100 -eni eth0 not vlan

если тегированный/не тегированный трафик

tcpdump –c 100 -eni eth0 vlan and not vlan 10 and not vlan 20 and not vlan 30

если тегированный трафик и известны нужные vlan

Оптимизация базы правил

Постоянно проверяйте базу правил на шлюзе (**удаляйте лишнее и смотрите за счетчиками**)

Постоянно проверяйте настройки и правила IPS (**убирайте не нужные проверки и добавляйте исключения**)

Постоянно проверяйте настройки и правила APCL/URLF (**убирайте не нужные проверки и добавляйте исключения**)

Оптимизация NGFW Palo Alto

Palo Alto Networks Performance Tuning (ESXi)

Лучшие практики по оптимизации (версии 8.0, 8.1 и 9.0)

- Включить поддержку **SR-IOV** для совместимых карт (ixgbe, i40e)
- Обновить **драйвера** для карт, совместимых с SR-IOV (например, карта от Intel 10G с драйвером ixgbe 4.4.1)
- Включить поддержку **DPDK** (нужен драйвер VMXNET3 или ixgbe, ixgbevf, i40e, i40evf)
- Включить поддержку **Multi-queue** на ESXi

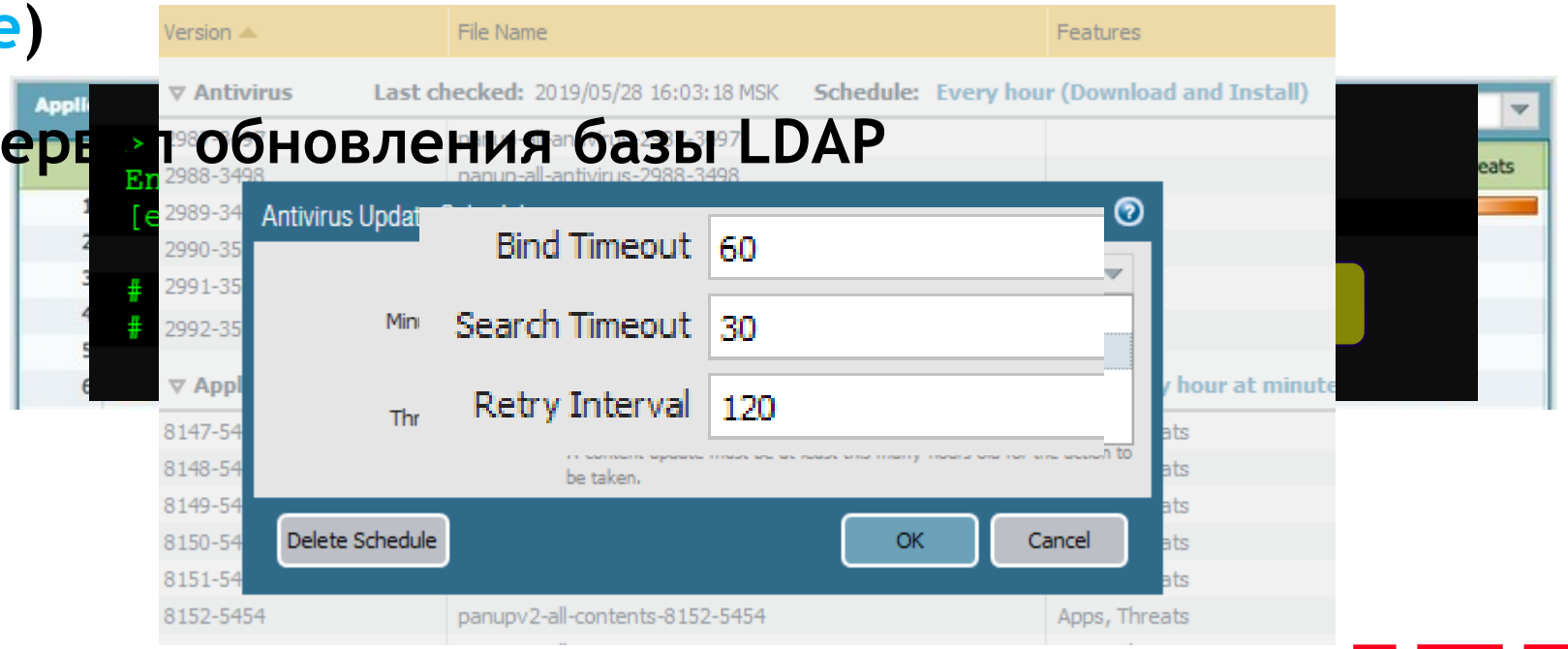
Необходима ESXi 6.0.0.0 или более новый версии

ITSF

Palo Alto Networks Performance Tuning (MP)

Лучшие практики по оптимизации (версии 8.0, 8.1 и 9.0)

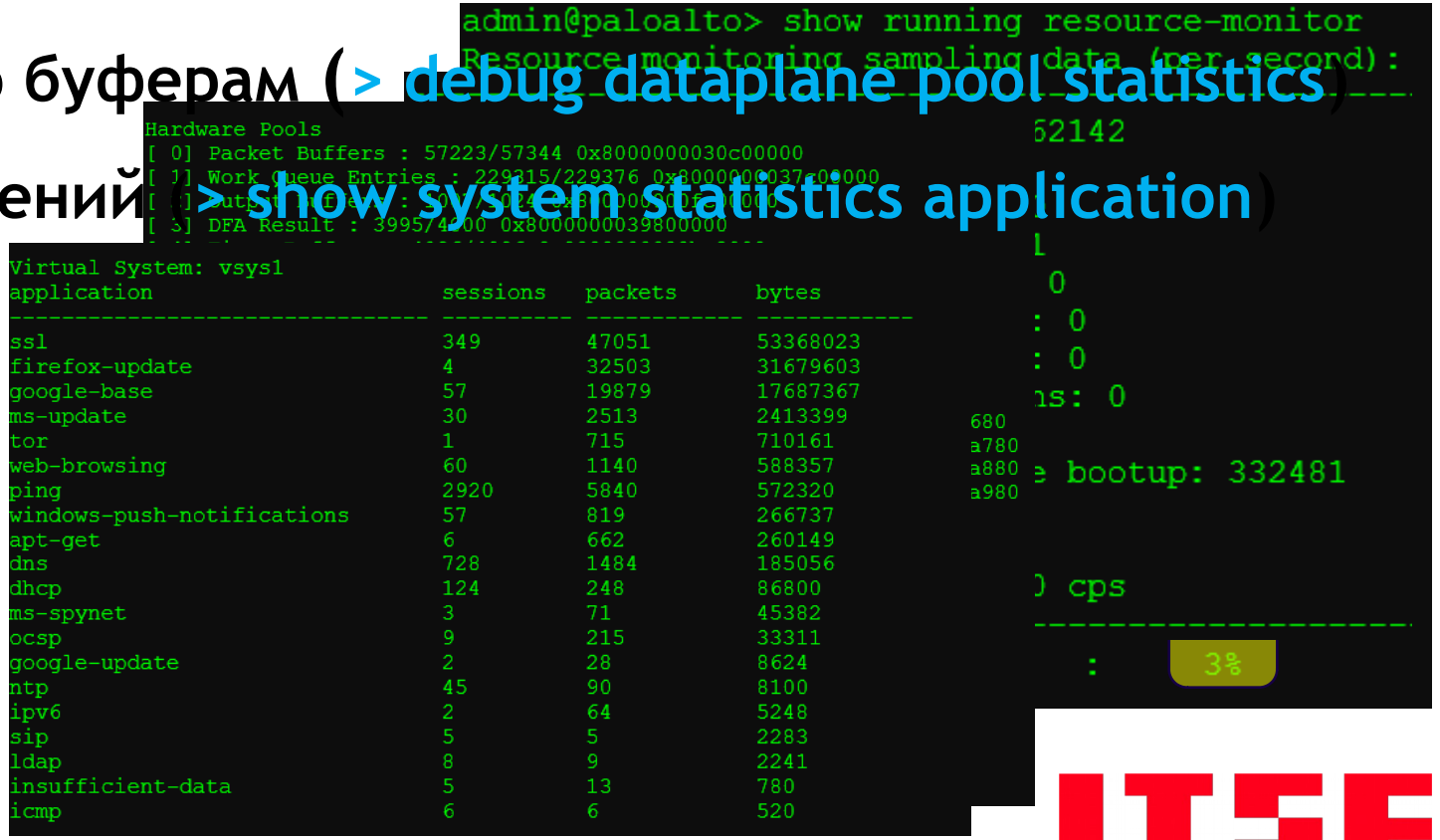
- Уменьшить количество регистрируемых событий (DNS, NetBios, Ping)
- Увеличить период обновления FQDN объектов
- Скорректировать параметры авто обновления сигнатур (AV, Apps & Treats, WildFire)
- Увеличить интервал обновления базы LDAP



Palo Alto Networks Performance Tuning (DP)

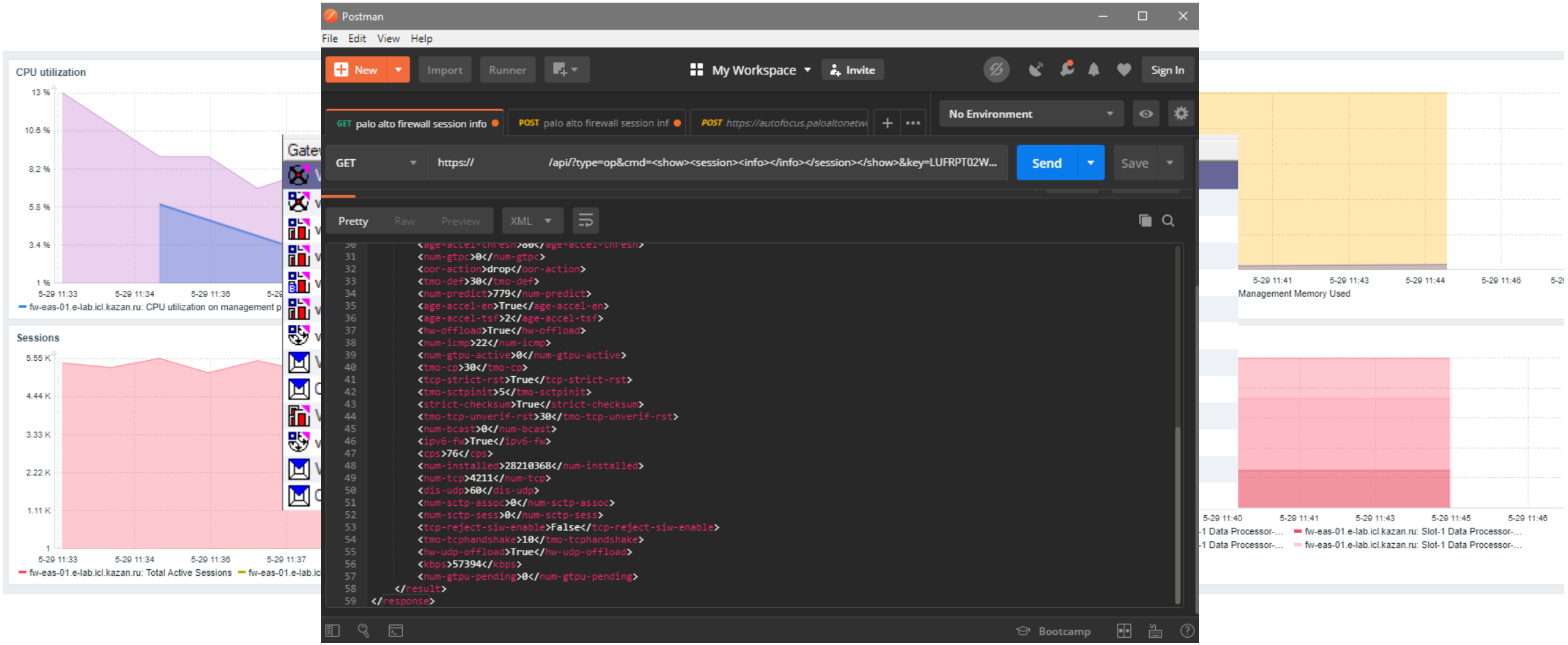
Лучшие практики по оптимизации (версии 8.0, 8.1 и 9.0)

- Посмотреть загрузку по модулям (> show running resource-monitor)
- Посмотреть статистику по текущим сессиям (> show session info)
- Посмотреть статистику по буферам (> debug dataplane pool statistics)
- Проверить Top-20 приложений (> show system statistics application)

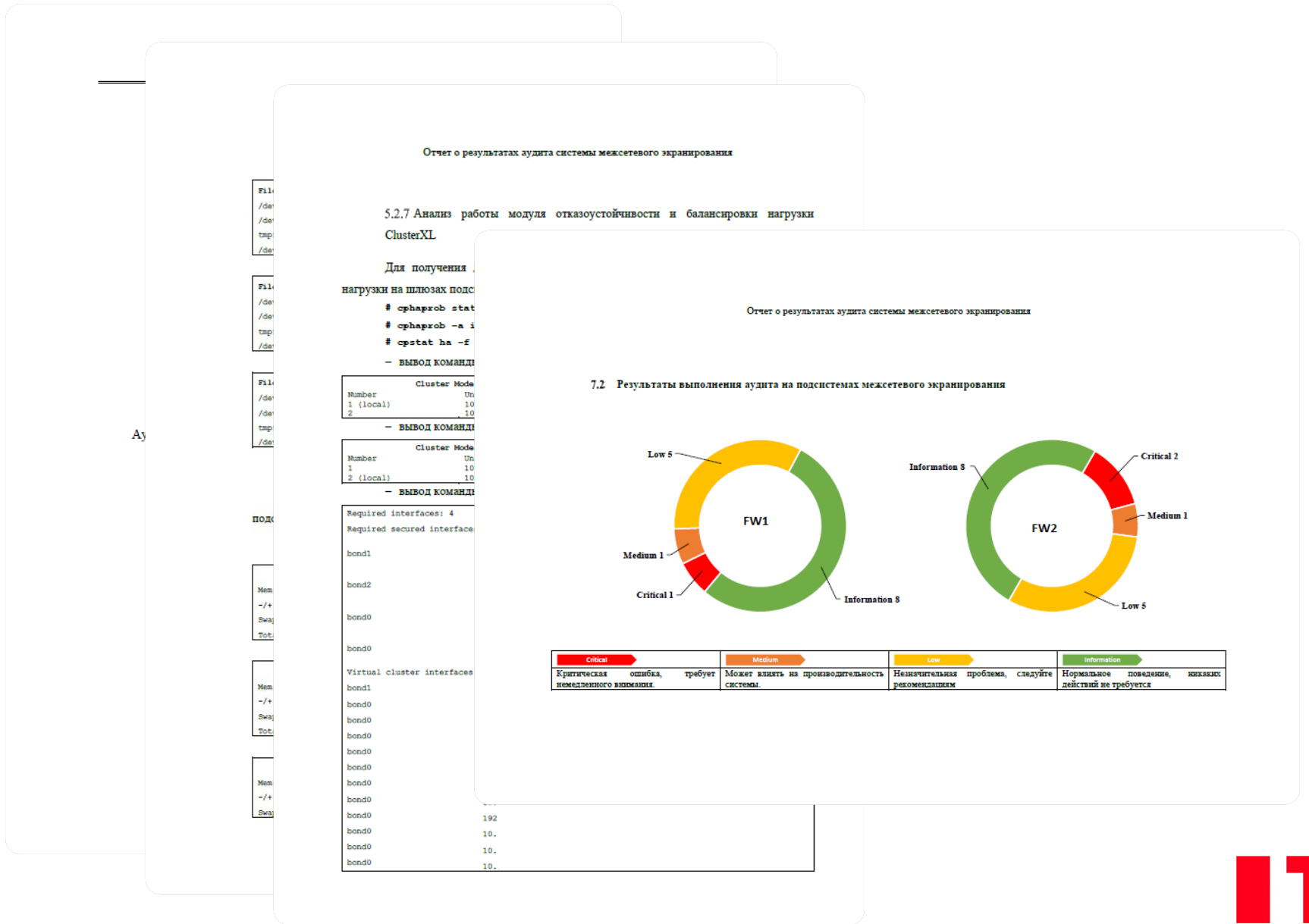


Как это всё отслеживать...?

Мониторинг показателей NGFW (пороговые значения)



Периодический аудит состояния шлюзов



Есть вопросы?

Задавайте!