The logo consists of the letters 'ITSEF' in a bold, white, sans-serif font. The letters are closely spaced and have a slightly irregular, blocky appearance.

ITSEF

ХІІІ ЦИФРОВОЙ ФОРУМ

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ РЕШЕНИЙ NGFW

Михаил Черкашин

Очень частая ситуация

Под проект был куплен межсетевой экран



Его настройка выполнялась только на старте проекта

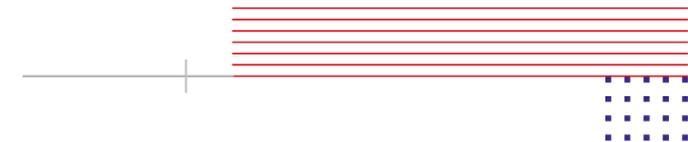
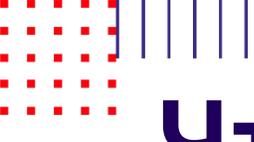


Сопровождение сводится к созданию новых правил



Текущий результат





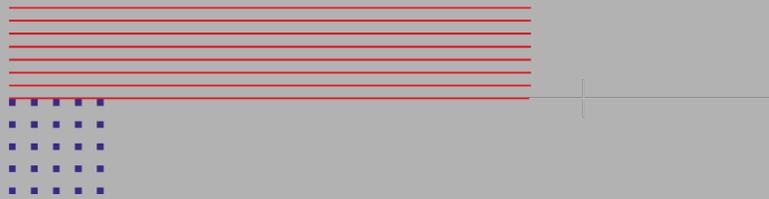
Что мы рассмотрим

Зачем производить оптимизацию

Что мы **можем** и **не можем** оптимизировать

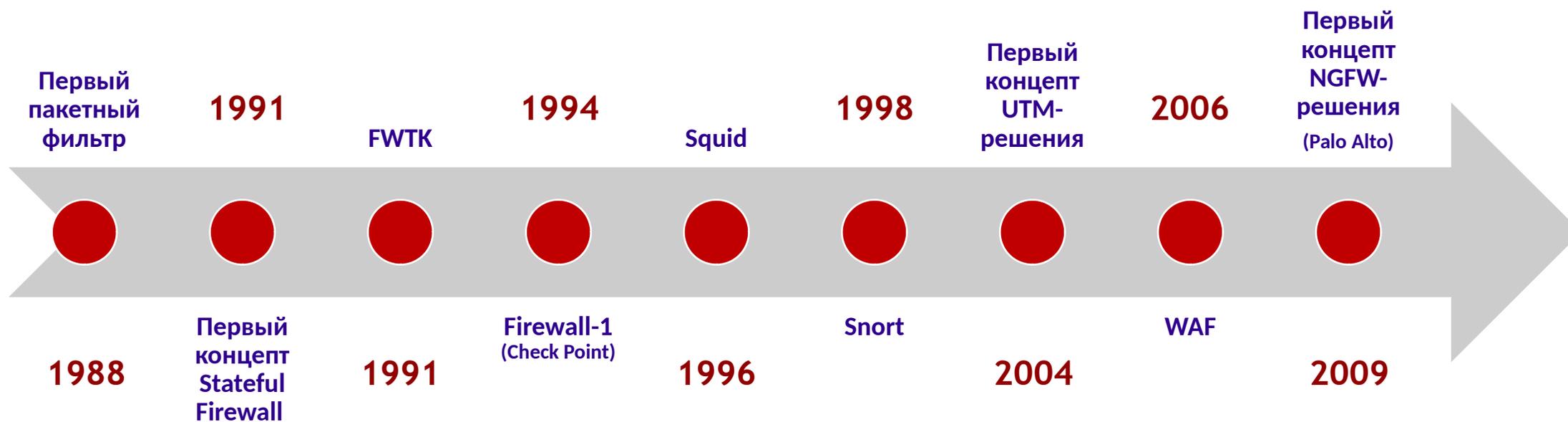
Как это всё отслеживать...

Зачем нужно что-то оптимизировать?



ITSEF

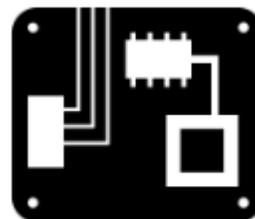
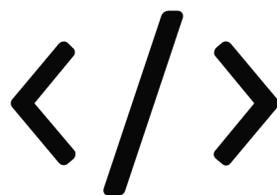
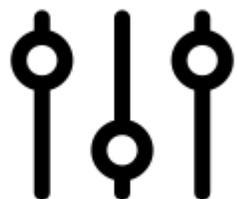
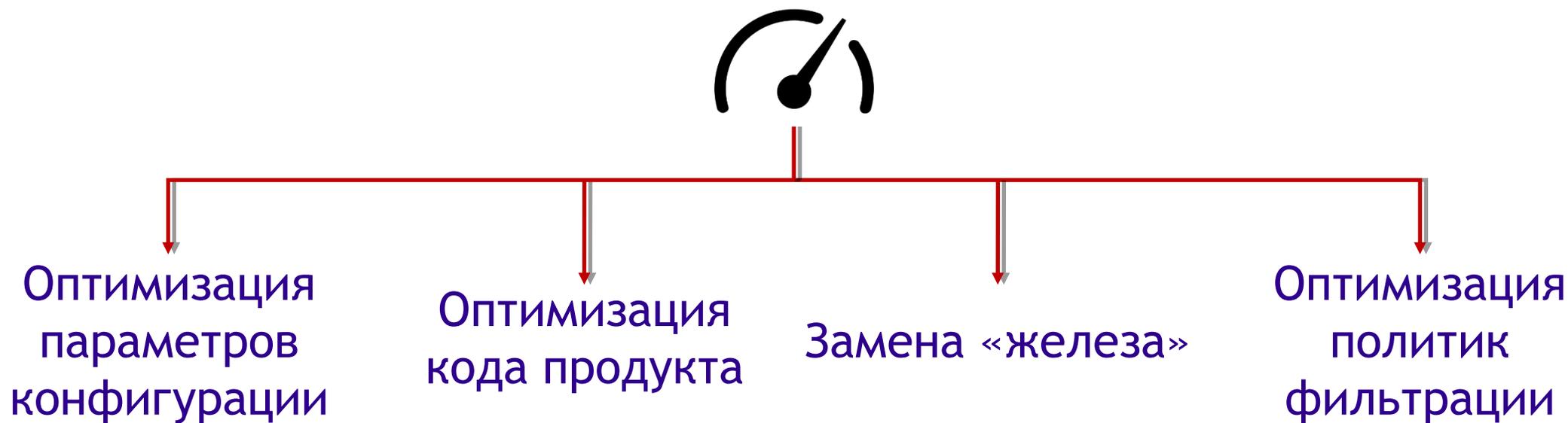
Эволюция межсетевого экрана



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

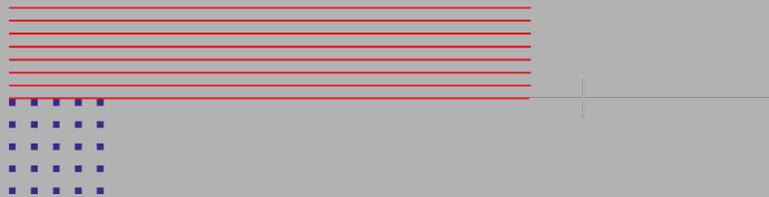


Долго и сложно

Дорого

ITSEF

Оптимизация NGFW Check Point



ITSEF

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**)

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



ITSEF

Palo Alto Networks Performance Tuning (ESXi)

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

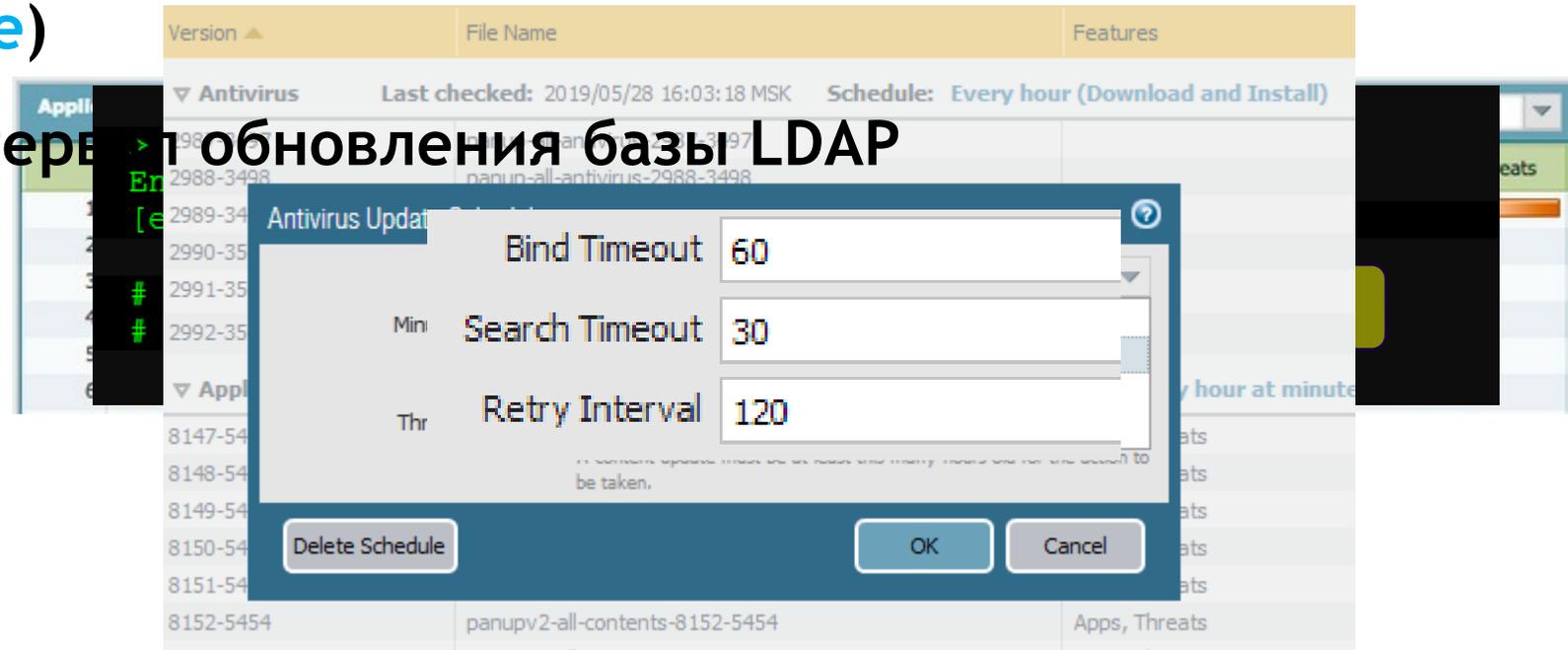
- Включить поддержку SR-IOV для совместимых карт (**ixgbe, i40e**)
- Обновить драйвера для карт, совместимых с SR-IOV (**например, карта от Intel 10G с драйвером ixgbe 4.4.1**)
- Включить поддержку DPDK (**нужен драйвер VMXNET3 или ixgbe, ixgbev, i40e, i40evf**)
- Включить поддержку Multi-queue на ESXi

Необходима ESXi 6.0.0.0 или более новой версии

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**)

```
admin@paloalto> show running resource-monitor
Resource monitoring sampling data (per second):
-----
Hardware Pools
[ 0] Packet Buffers : 57223/57344 0x80000000030c00000 52142
[ 1] Work Queue Entries : 229215/229376 0x80000000033700000
[ 2] Output Buffers : 512/248 0x0000000000000000
[ 3] DFA Result : 3995/4000 0x80000000039800000
-----

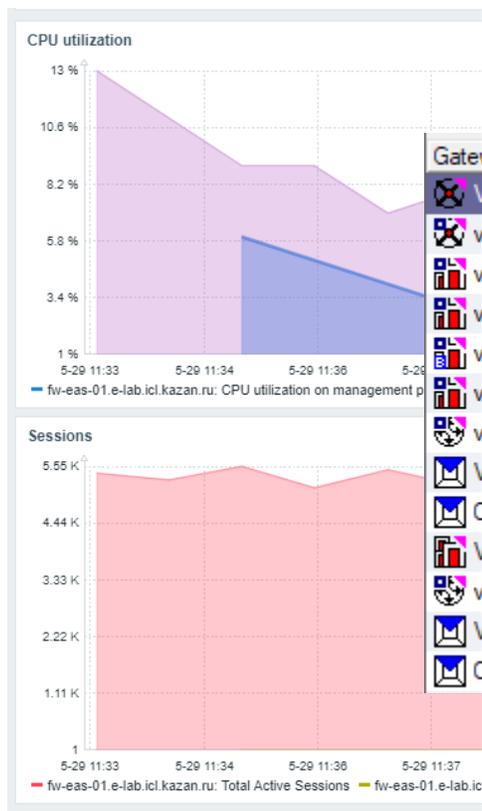
Virtual System: vsys1
application          sessions  packets  bytes
-----
ssl                  349      47051   53368023
firefox-update      4         32503   31679603
google-base         57        19879   17687367
ms-update           30        2513    2413399
tor                  1          715     710161
web-browsing        60         1140    588357
ping                 2920       5840    572320
windows-push-notifications 57         819     266737
apt-get              6           662     260149
dns                  728        1484    185056
dhcp                 124         248     86800
ms-spyntet          3           71      45382
ocsp                 9           215     33311
google-update       2            28      8624
ntp                  45           90      8100
ipv6                  2            64     5248
sip                   5            5      2283
ldap                  8            9      2241
insufficient-data   5            13       780
icmp                  6            6       520

: 0
: 0
ns: 0
680
a780
a880 = bootup: 332481
a980
) cps
-----
: 3%
```



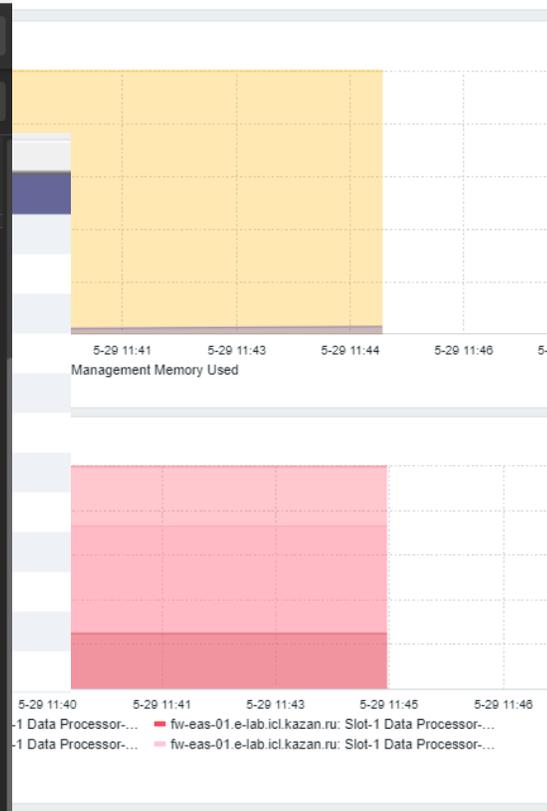
Как это всё отслеживать...?

Мониторинг показателей NGFW (пороговые значения)



The screenshot shows the Postman interface. The active request is a GET call to `https://[redacted]/api?type=op&cmd=<show><session><info></info></session></show>&key=LUFRPT02W...`. The response is displayed in the 'Pretty' view as an XML document:

```
<age-accel-cmres>0</age-accel-cmres>
<num-gtpe>0</num-gtpe>
<oor-action>drop</oor-action>
<tmo-def>30</tmo-def>
<num-predict>779</num-predict>
<age-accel-en>True</age-accel-en>
<age-accel-ts>2</age-accel-ts>
<hw-offload>True</hw-offload>
<num-icmp>22</num-icmp>
<num-gtpe-active>0</num-gtpe-active>
<tmo-cp>30</tmo-cp>
<tcp-strict-rst>True</tcp-strict-rst>
<tmo-sctpinit>5</tmo-sctpinit>
<strict-checksum>True</strict-checksum>
<tmo-tcp-unverif-rst>30</tmo-tcp-unverif-rst>
<num-bcast>0</num-bcast>
<ipv6-fw>True</ipv6-fw>
<cps>76</cps>
<num-installed>28210368</num-installed>
<num-tcp>4211</num-tcp>
<dis-udp>60</dis-udp>
<num-sctp-assoc>0</num-sctp-assoc>
<num-sctp-sess>0</num-sctp-sess>
<tcp-reject-siw-enable>False</tcp-reject-siw-enable>
<tmo-tcphandshake>10</tmo-tcphandshake>
<hw-udp-offload>True</hw-udp-offload>
<kbps>57394</kbps>
<num-gtpe-pending>0</num-gtpe-pending>
</result>
</response>
```



Периодический аудит состояния шлюзов

Отчет о результатах аудита системы межсетевого экранирования

5.2.7 Анализ работы модуля отказоустойчивости и балансировки нагрузки ClusterXL

Для получения
нагрузки на шлюзах подс

```
# srgprob stat
# srgprob -a i
# srstat ha -f
- ВЫВОД КОМАНД
```

```
Cluster Mode
Number Un
1 (local) 10
2 10
- ВЫВОД КОМАНД
```

```
Cluster Mode
Number Un
1 10
2 (local) 10
- ВЫВОД КОМАНД
```

Required interfaces: 4
Required secured interface:

bond1

bond2

bond0

bond0

Virtual cluster interfaces

bond1

bond0

bond0

bond0

bond0

bond0

bond0

bond0

bond0 192

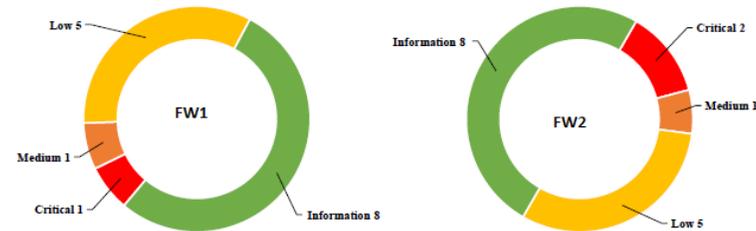
bond0 10.

bond0 10.

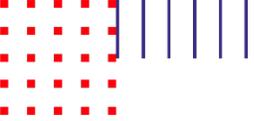
bond0 10.

Отчет о результатах аудита системы межсетевого экранирования

7.2 Результаты выполнения аудита на подсистемах межсетевого экранирования



Critical	Medium	Low	Information
Критическая ошибка, требует немедленного внимания.	Может влиять на производительность системы.	Незначительная проблема, следуйте рекомендациям.	Нормальное поведение, никаких действий не требуется.



Есть вопросы?

Задавайте!