

Виртуализация криптокоммутаторов Континент в среде Oracle VirtualBox

А. С. Коваль

ВГУ, ФКН, каф. ИС

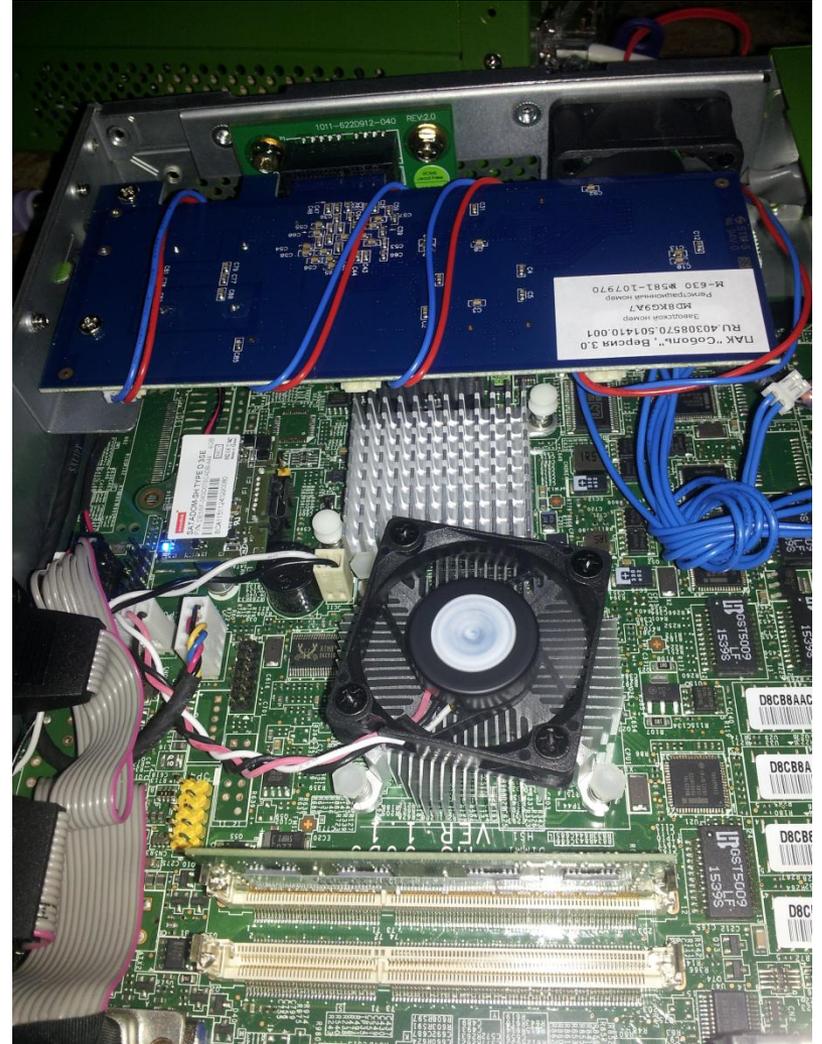
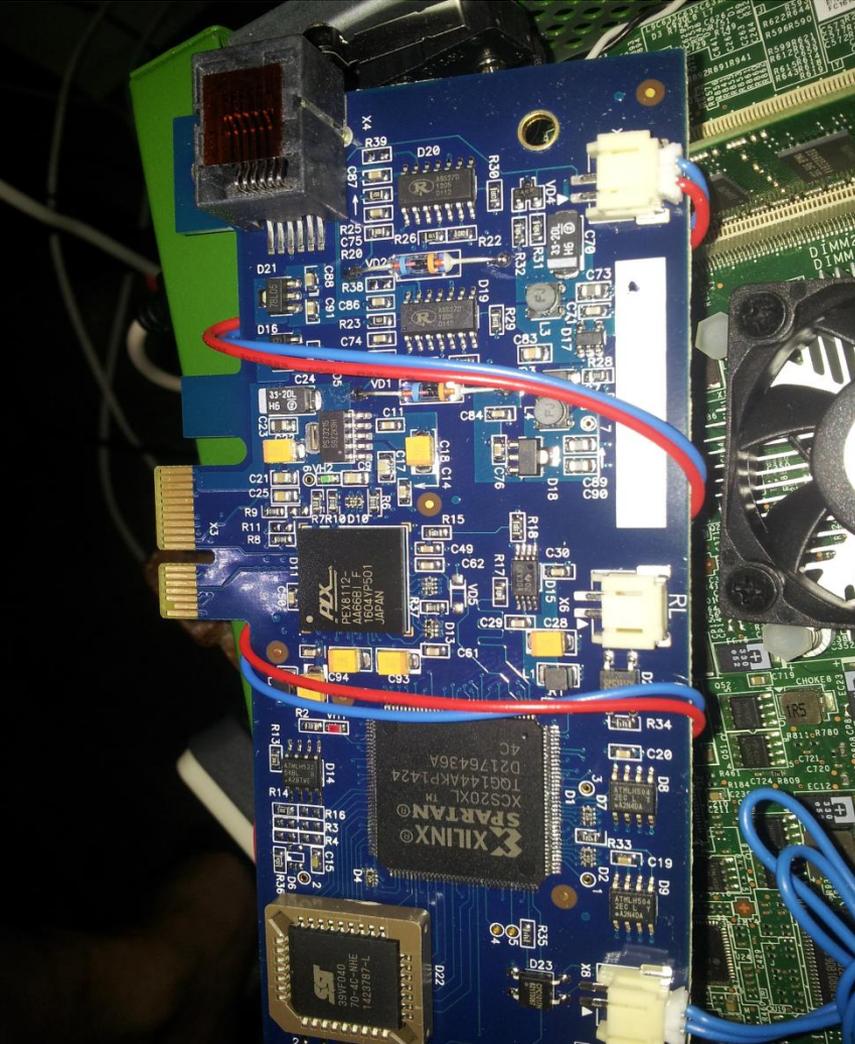
Виртуализация сетевых инфраструктур

- Виртуализация сетевых инфраструктур – формирование сети в виртуальной среде, например, в Oracle Virtual Box
- Цель виртуализации в данном случае – создание стенда для исследования возможностей, определения характеристик аппаратно-программных комплексов шифрования, в частности, «АПКШ Континент» компании «Код Безопасности»
- Также, целями могут быть: демонстрация правильного/штатного применения заказчиком, формирование полностью программной реализации для размещения «в облаке», как рабочий инструмент (отдельный продукт).
- Виртуализация сетевых инфраструктур в учебных целях используется на ФКН широко и обсуждалась, в частности, на прошлой конференции IPMT-2020 .
- Однако особенности виртуальных сред накладывают некоторые ограничения на функции виртуализированного оборудования, а иногда и изменяют сами функции.
- Рассматриваются особенности поведения и характеристики пропускной способности виртуализированного аппаратно-программного комплекса шифрования (АПКШ) «Континент» ООО «Код Безопасности» в среде Oracle Virtual Box.

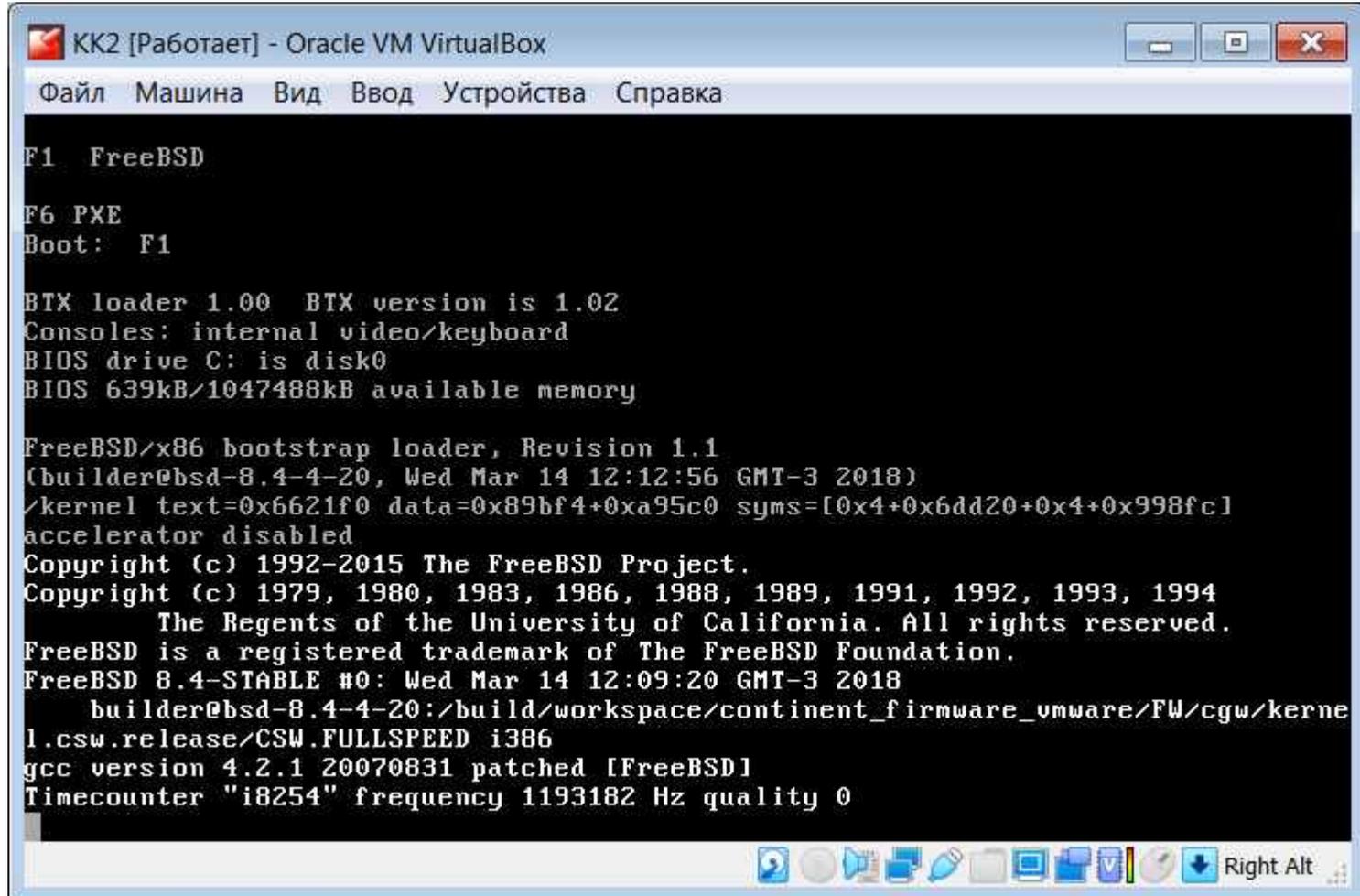
АПКШ Континент



АПКШ КОНТИНЕНТ



Начальная загрузка «Континента»



The image shows a screenshot of a Virtual Machine window titled "KK2 [Работает] - Oracle VM VirtualBox". The window contains a terminal window displaying the boot process of FreeBSD. The text in the terminal is as follows:

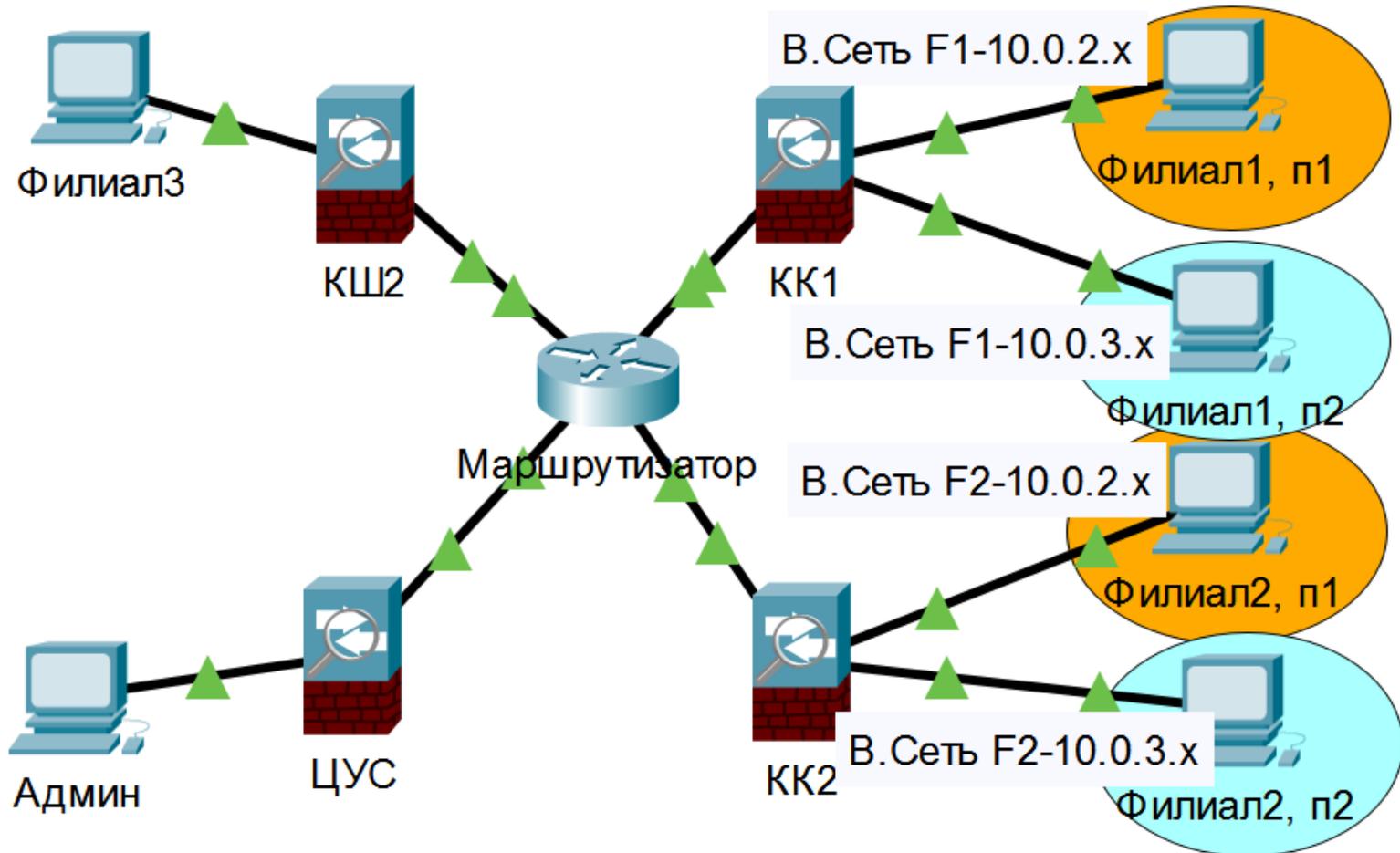
```
F1 FreeBSD
F6 PXE
Boot: F1

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 639kB/1047488kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
(builder@bsd-8.4-4-20, Wed Mar 14 12:12:56 GMT-3 2018)
/kernel text=0x6621f0 data=0x89bf4+0xa95c0 syms=[0x4+0x6dd20+0x4+0x998fc]
accelerator disabled
Copyright (c) 1992-2015 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
FreeBSD is a registered trademark of The FreeBSD Foundation.
FreeBSD 8.4-STABLE #0: Wed Mar 14 12:09:20 GMT-3 2018
    builder@bsd-8.4-4-20:/build/workspace/continent_firmware_vmware/FW/cgw/kerne
l.csw.release/CSW.FULLSPEED i386
gcc version 4.2.1 20070831 patched [FreeBSD]
Timecounter "i8254" frequency 1193182 Hz quality 0
```

The window also shows a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". At the bottom, there is a taskbar with various system icons and a "Right Alt" button.

Топология сети для L2-3VPN



Виртуальные машины и снэпшоты

The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a list of virtual machines is displayed, including SNS, ARM, CUS, KSH-main, Router, AP, WS1, and KK2 (which is currently running). The main area shows the snapshot tree for the selected VM, 'KK2 загружен'. The tree includes a root snapshot 'Текущее состояние (изменено)' and two child snapshots: 'Выложено на G-drive' and 'появился в ЦУС'. The 'появился в ЦУС' snapshot has a sub-snapshot 'KK2 загружен'. The bottom right pane shows the 'Информация' tab for the selected snapshot, displaying its name and description.

Имя	Дата создания
Выложено на G-drive	15.05.2020 8:51
появился в ЦУС	25.01.2021 0:00 (16 часов назад)
KK2 загружен	25.01.2021 0:35 (15 часов назад)

Атрибуты Информация

Имя: KK2 загружен

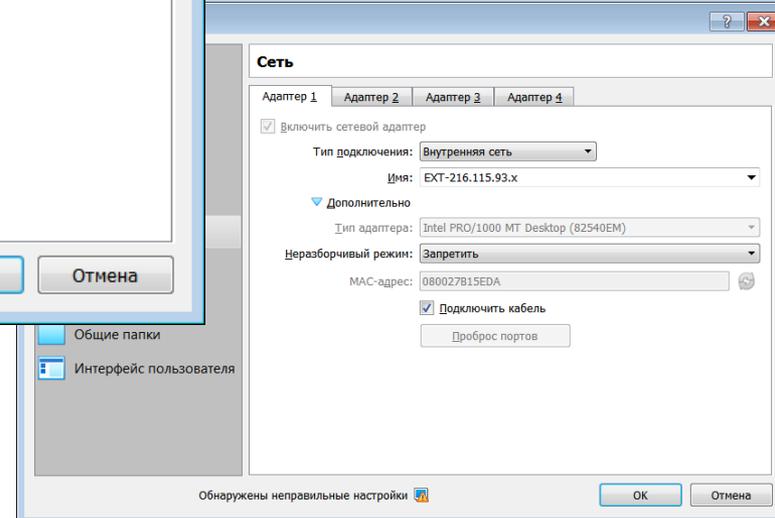
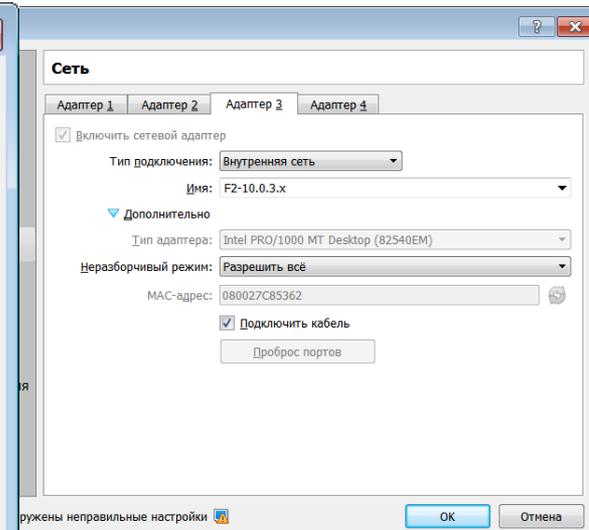
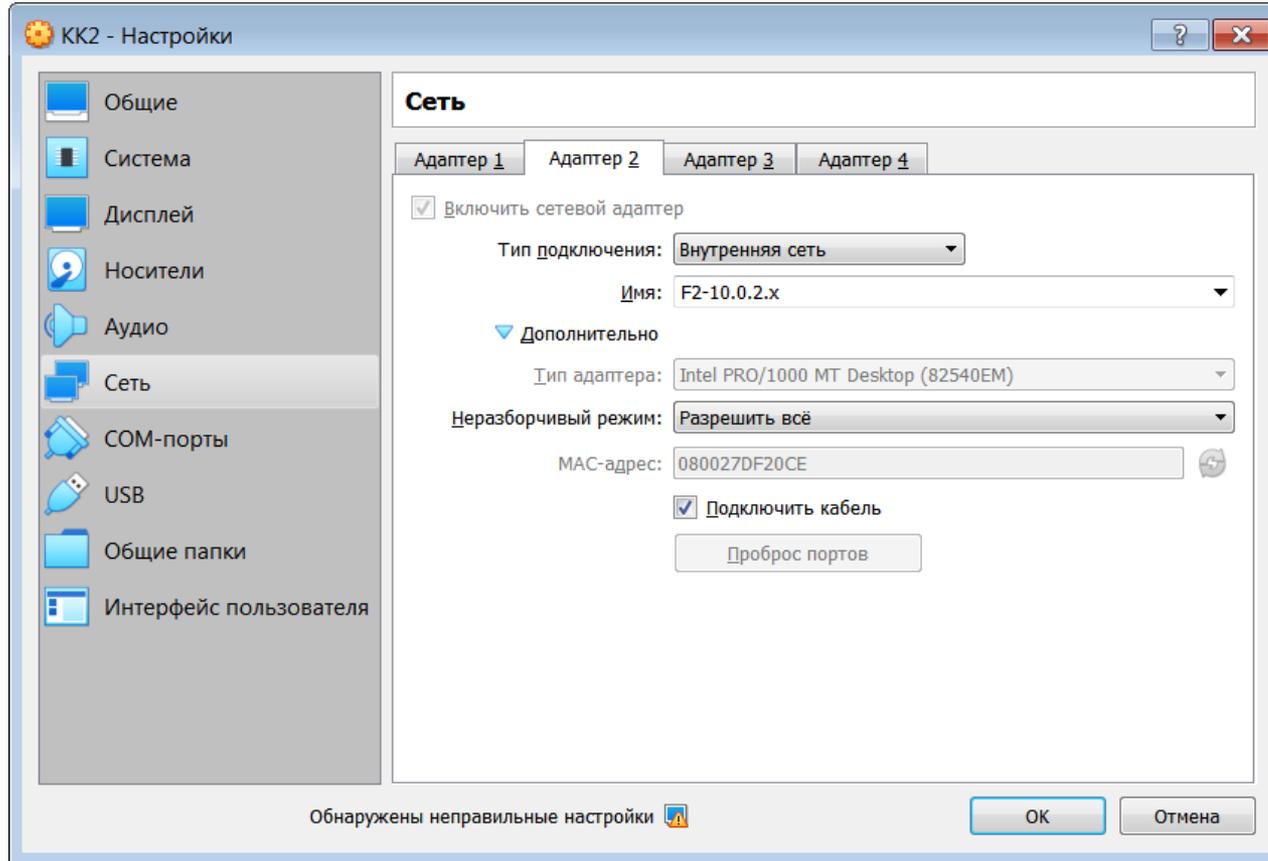
Описание: KK2 загружен, порты в 2,3,4 сети F2

Применить Сбросить

Режимы работы портов криптокоммутаторов

- L2VPN трафик в такой конфигурации не будет проходить через криптокоммутаторы
- Оборудование в отличие от хостов вполне может принимать кадры с MAC-адресом назначения, отличающимся от адреса интерфейса, в частности, для порта криптокоммутатора – это обычный режим
- Необходим «неразборчивый» режим работы порта, обращенного в сторону конечной сети

Виртуальные сети филиалов и режим работы портов КК1,2



ПУ ЦУС и криптокоммутаторы

Континент - Главный администратор

Объекты Вид ЦУС Операции Справка

Все объекты

- Центр Управления Сетью
 - Сетевые объекты
 - Группы сетевых объектов
 - Сервисы
 - Пользователи
 - Временные интервалы
 - Классы трафика
 - Реакции на события
 - Сертификаты
 - Правила фильтрации
 - База решающих правил
 - Виртуальные коммутаторы
 - Администраторы
 - Сетевые устройства Континент
 - Криптошлюзы
 - Криптокоммутаторы**
 - Детекторы атак
 - Отчёты
 - Внешние криптографические сети

Криптокоммутаторы

Название	Описание	Состояние	НСД	NAT	Кластер	Multi-WAN	Каналы VPN
KK1		Включен				✓ RT	
KK2		Включен				✓ RT	

Состояние КК

KK1

Включен: **ДА**

Введен в эксплуатацию: **ДА**

Ключи КК: **действуют до 31.12.1970 22:03:25**

Запланированное время смены ключей КК: **Никогда**

Зарегистрированы события НСД: **НЕТ**

Мягкий режим пакетного фильтра: **НЕТ**

Статус автозагрузки: **НЕТ**

Каналы VPN

Связь	Количество неработоспособных каналов	Время отказа
KK1 <-> KK2		

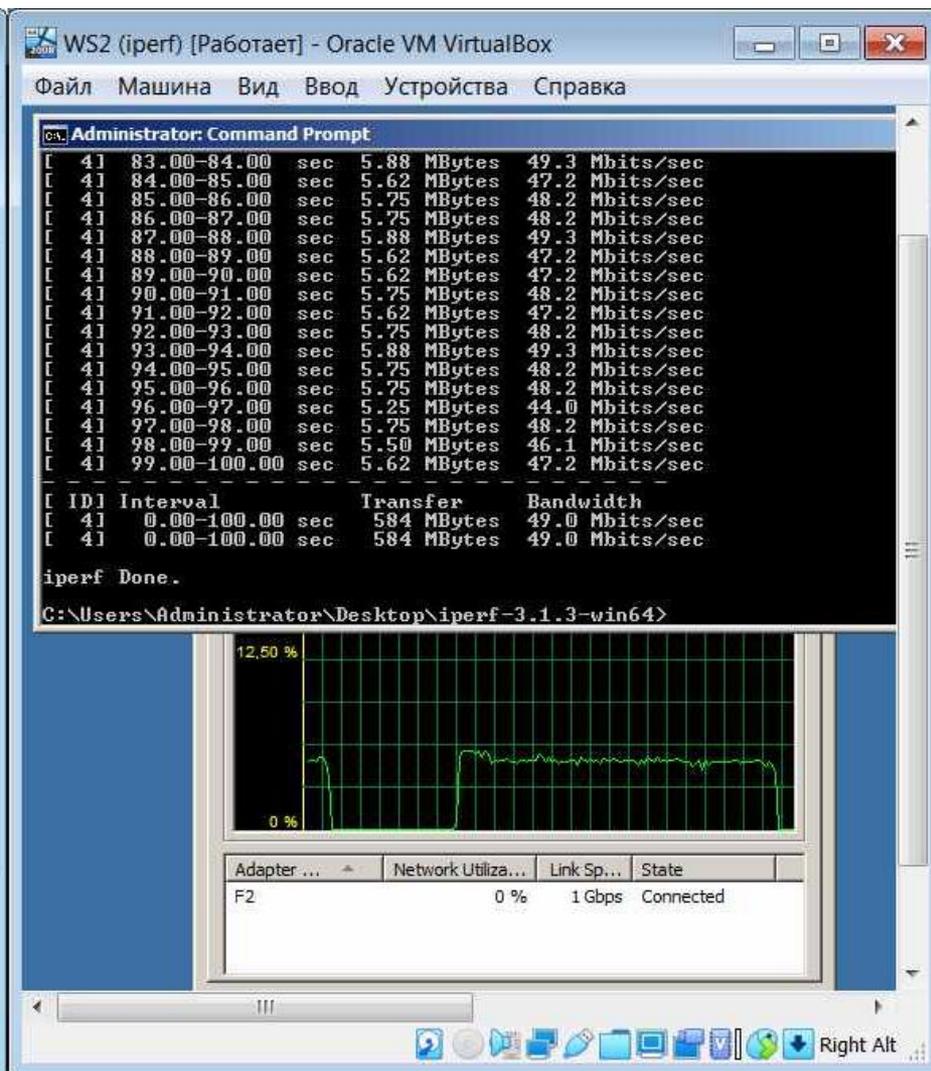
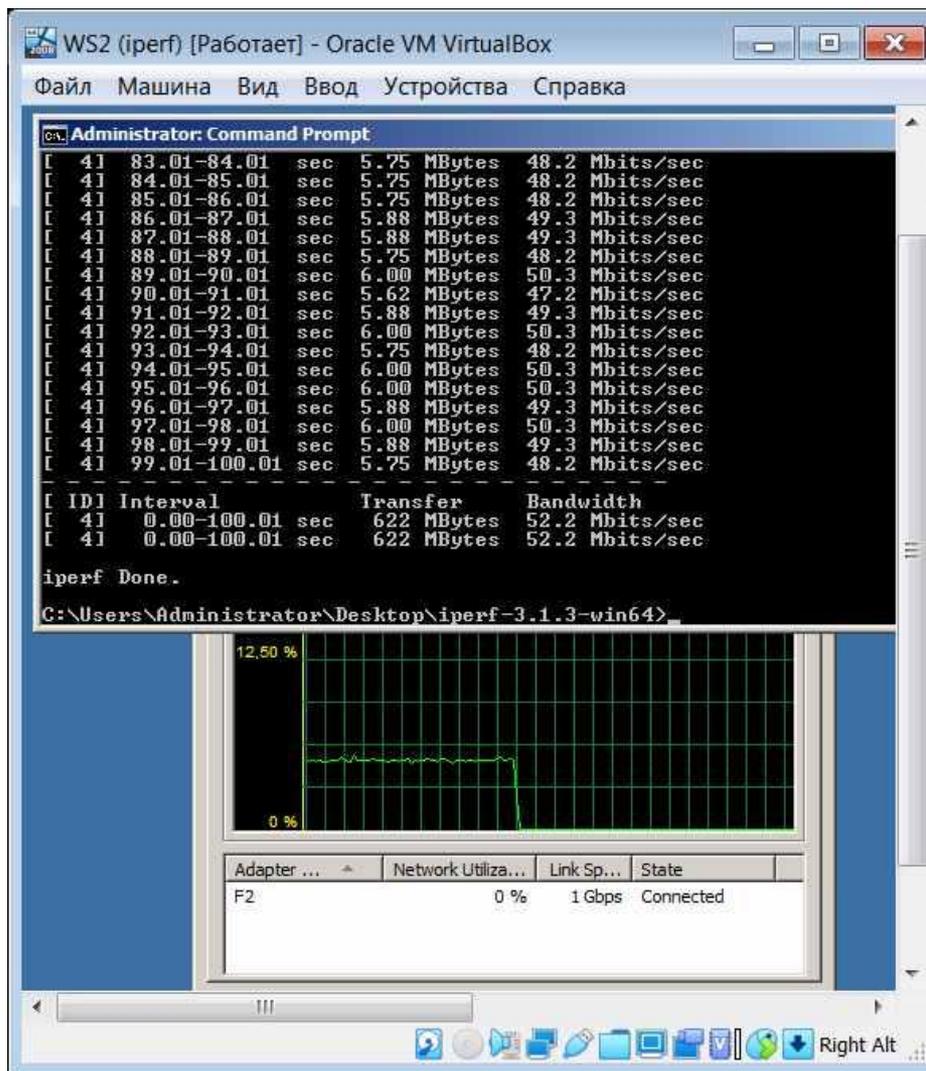
Статистика по трафику

Интерфейс	Количество байт		Количество пакетов	
	входящих	исходящих	входящих	исходящих
Всего	2 111 005 940	2 105 327 696	1 826 601	1 826 675
em0	2 083 028 771	55 028 259	1 360 368	468 496
em1	27 977 169	2 050 299 191	466 233	1 358 176

Состояние КК | Виртуальные коммутаторы | Очередь заданий

0 0 3/3

Пропускная способность L2VPN инфраструктуры



Пропускная способность L3VPN и дамп трафика

WS2 (iperf) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройство Справка

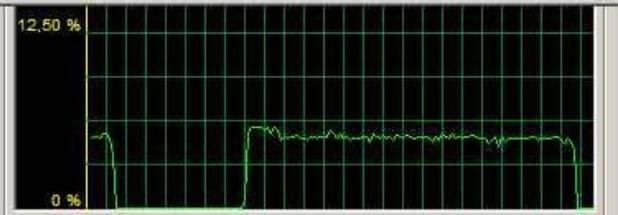
Administrator: Command Prompt

```
[ 41] 83.00-84.00 sec 5.88 MBytes 49.3 Mbits/sec
[ 41] 84.00-85.00 sec 5.62 MBytes 47.2 Mbits/sec
[ 41] 85.00-86.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 86.00-87.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 87.00-88.00 sec 5.88 MBytes 49.3 Mbits/sec
[ 41] 88.00-89.00 sec 5.62 MBytes 47.2 Mbits/sec
[ 41] 89.00-90.00 sec 5.62 MBytes 47.2 Mbits/sec
[ 41] 90.00-91.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 91.00-92.00 sec 5.62 MBytes 47.2 Mbits/sec
[ 41] 92.00-93.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 93.00-94.00 sec 5.88 MBytes 49.3 Mbits/sec
[ 41] 94.00-95.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 95.00-96.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 96.00-97.00 sec 5.25 MBytes 44.0 Mbits/sec
[ 41] 97.00-98.00 sec 5.75 MBytes 48.2 Mbits/sec
[ 41] 98.00-99.00 sec 5.50 MBytes 46.1 Mbits/sec
[ 41] 99.00-100.00 sec 5.62 MBytes 47.2 Mbits/sec
```

ID	Interval	Transfer	Bandwidth
[41]	0.00-100.00 sec	584 MBytes	49.0 Mbits/sec
[41]	0.00-100.00 sec	584 MBytes	49.0 Mbits/sec

iperf Done.

C:\Users\Administrator\Desktop>iperf-3.1.3-win64>



Adapter	Network Utilization	Link Speed	State
F2	0 %	1 Gbps	Connected

*OPT2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol
11432	2.272785	196.115.92.1	216.115.92.1	UDP
11433	2.272788	196.115.92.1	216.115.92.1	UDP
11434	2.272791	196.115.92.1	216.115.92.1	UDP
11435	2.272794	196.115.92.1	216.115.92.1	UDP

Frame 11434: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

- Ethernet II, Src: PcsCompu_fd:be:1b (08:00:27:fd:be:1b), Dst: PcsCompu_a3:00:00:00:00:00
- Internet Protocol Version 4, Src: 196.115.92.1, Dst: 216.115.92.1
- User Datagram Protocol, Src Port: 10000, Dst Port: 10000
 - Source Port: 10000
 - Destination Port: 10000
 - Length: 1480
 - [Checksum: [missing]]
 - [Checksum Status: Not present]
 - [Stream index: 0]
- Data (1472 bytes)
 - Data: 01000000004ada5b000000005a23c27a5aff587340002500...
 - [Length: 1472]

```
0000 08 00 27 a3 19 dd 08 00 27 fd be 1b 08 00 45 00  ..'.....'.....E
0010 05 dc 6f 6a 40 00 3f 11 71 bd c4 73 5c 01 d8 73  ..oj@.? q...s\..s
0020 5c 01 27 10 27 10 05 c8 00 00 01 00 00 00 00 4a  \.....]
0030 da 5b 00 00 00 00 5a 23 c2 7a 5a ff 58 73 40 00  .[....Z# zZ Xs@
0040 25 00 e4 1e 2e 5d b1 d7 4b 62 50 29 33 f6 40 f5  %....]..Kbp)3@
0050 24 0a 5a e8 8f c2 73 d3 bd 2c 73 51 cd 26 81 25  $Z...s...sQ&X
0060 9c 7c fc ac 69 5e de cf 3e 39 38 4d ac da 7e a5  .|..i^>98M~
0070 e0 2f 30 c5 f4 a1 eb 21 e2 00 16 ac ec 2f 86 5d  /0...! .../
0080 f0 21 8d 15 78 59 55 18 c9 f8 9a 5c fb 0f fd a0  .!..xYU... \
0090 c8 77 d2 0f 9f 88 77 64 03 d7 7b ef ff 49 f2 17  .w...wd...{..I
00a0 48 00 45 f1 51 40 04 66 4d 4e 04 0f 00 00 46 f1  .H...}...f
```

wires...capn Packets: 15914 · Displayed: 15914 (100.0%) · Dropped: 1366 (8.6%) Profile: Def

Заключение

- Рассматривались особенности реализации инфраструктуры защищенной сети в виртуальной среде Oracle Virtual Box.
- Определены пропускные способности L2 и L3 VPN реализаций, особенности режимов портов виртуальных интерфейсов для криптокоммутаторов.
- Планируется оценить возможность применения виртуализированного оборудования для обработки реального трафика, обеспечив большой процессорный ресурс узлам, на которых выполняются криптопреобразования.