Инцидент № СООО1

Дата создания: 21.07.2021

Дата последней корректировки: ___26.01.2022_

Инструкция по реагированию на инциденты, решением которых является переустановка или установка dst файла на Coordinator.

Этап 1. Подготовка оборудования.

Для установки/переустановки dst файла потребуется:

- Физический доступ к Coordinator HW
- Питание к Coordinator HW
- Монитор с VGA разъемом
- Питание к монитору
- Клавиатура
- Кабель VGA
- USB-flash накопитель в формате FAT32, ext2, ext3 или ext4.

Этап 2. Настройка координатора

Этап 2.1. Сброс ключевой информации координатора¹

При запуске Coordinator HW операционная система запросит логин и пароль. Слева от login имя координатора, данное ему при предыдущей установке. При вводе пароля символы не отображаются.

Login	user
Password	«в .xps файле»



Рисунок 1

После успешной авторизации под user, требуется повысить права командой *enable*. Потребуется ввести пароль администратора. Если он Вам неизвестен, то уточните его у Администратора сети. После успешного повышения прав ">" заменяется на "#".

hw–va–10e9000d login: user	
Password:	
Last login: Wed Jun 9 21:38:59 +05 2021 on tty1	
Loading command shell, please wait	
Starting the command line interface of Platform:	VA VMWARE
hw—va—10e9000d> enable	
Type the administrator password:	
hw—va—10e9000d#	

Рисунок 2

Для удаления ключевой информации необходимо ввести команду *admin remove keys*. Далее на экране отобразится предупреждающее сообщение. Для продолжения удаления необходимо согласиться с заглавной буквы (Yes).

¹ Данный этап пропускается в случае, если Ваш корд был получен вами после ремонта. Приступите к настройке сразу с этапа 2.2.

hw-va-10e9000d login: user Password: Last login: Wed Jun 9 21:38:59 +05 2021 on tty1 Loading command shell, please wait... Starting the command line interface of Platform: VA VMWARE hw-va-10e9000d> enable Type the administrator password: hw-va-10e9000d# admin remove keys This command deletes all VPN keys and cannot be reverted, You will need to deploy keys anew after executing this command. Are you sure you want to execute this command? Continue? [Yes/No]: Yes_

Рисунок З

После согласия начнется процесс удаления.

Last login: Wed Jun 9 21:38:59 +05 2021 on tty1 Loading command shell, please wait... Starting the command line interface of Platform: VA VMWARE hw-va-10e9000d> enable Type the administrator password: hw-va-10e9000d# admin remove keys This command deletes all VPN keys and cannot be reverted, You will need to deploy keys anew after executing this command. Are you sure you want to execute this command? Continue? [Yes/No]: Yes Stopping all VPN services Shutting down failover daemon Shutting down ViPNet Web GUI service Shutting down MFTP daemon Shutting down Alg daemon Shutting down IpLir Unloading IpLir driver Unloading watchdog driver Module l2overip is already deconfigured Loading VPN modules Removing key–disk directory Pretending to unload VPN modules Unloading VPN modules Removing iplirpsw... Reseting and stopping services... UPS service is disabled NTP server is already STOPPED DNS server is already STOPPED DHCP relays are already STOPPED DHCP server is already STOPPED Stopping Quagga monitor daemon: (waiting) .. watchquagga. Stopping Quagga daemons (prio:0): zdhcpd (waiting) .

Рисунок 4

После успешного удаления система может перезагрузиться и запросить login как в начале следующего этапа. Если все произошло успешно, можно переходить к Этапу 2.2.

Этап 2.2. Настройка координатора с нуля.

При первоначальной инициализации координатора или после удаления ключевой информации координатор имеет базовое имя и базовую пару логин-пароль. Стоит отметить, что имя

координатора по умолчанию зависит от модели.

Product: ViPNet Coordinator VA Platform: VA VMWARE Software version: 4.3.3–4088 (C) JSC InfoTeCS, 2020; website: www.infotecs.ru, email: soft@infotecs.ru; phone (Russia): 8 800 250–0–260, phone (Moscow): +7 4 95 737–61–92 va login:

Рисунок 5

Login	user
Password	user

После успешной авторизации система предоставит на выбор два варианта настройки координатора:

- 1. В командой строке
- 2. Псевдографический интерфейс

В данной инструкции используется второй вариант. Для выбора достаточно ввести соответствующую цифру.



Рисунок 6

Дальнейшие действия будут в соответствии со скриншотами. В необходимых случаях будут даны комментарии.

VIPNET Key Setup (Use Pgup Pgubun to View the license)
ЛИЦЕНЗИОННОЕ СОГЛАЩЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ НА ИСПОЛЬЗОВАНИЕ ПО VIPNET COORDINATOR НИ 4 Настоящее соглашение заключается между Вами, Конечным пользователем, и ОАО "ИнфоТеКС" (OFPH: 1027739185066, ИНН: 7710013769, юридический адрес: 127287, г. Москва, Старий Петровско-Разумовский проезд, дои 1/23, стр. 1) и содержи информацию об авторском праве и объёме неисслачительных прав использования ПО VIPNET Coordinator HH 4. В случае несогласия с изложенными ниже условиями соглашение считается не закличенным, и Вы не вправе использовать П VIPNet Coordinator HH 4. Использование ПО VIPNet Coordinator HH 2 объем неисслачает Какличенным, и Вы не вправе использовать П VIPNet Coordinator H4. И спользование ПО VIPNet Coordinator H4 6 объемо безоговорочное принятие нестоящего соглашения и готовность нести ответственность в случае его нарушения в соответствии с нормами
 Определение понятий Порграмма для 36М - представленная в объективной чорме совокупность данных и команд, предназначенных для «унскционирования 36М и других компьютерных устройств в целях получения поределенного результата, а также эксплуатационная документация, предоставляемая в печатном и в электронном виде. Поограмма собеспечение VIPNet Coordinator HW 4 (ПО) - программа для 35М, производимая ОбО "ИнфоТекС", предустановленняя на программно-аппаратном компликсе VIPNet Coordinator HW 4. Оно "ИнфоТекС" (Правообладатель) - обладатель искличительных и имущественных авторских прав на ПО. Все авторские права на ПО защищены законодатель тово И Российской Ведерации о правах на результата интеллектуальной деятельности. По является интеллектуальной собственностью ОнО "ИнфоТекС". Конечный Пользователь с мидищены законо ими изическое лиць, использущие (намереважцеся использовать) ПО для собственных (производственных) нука. Система регистрации легальных пользователей ПО. Конечный Пользователь с воими изическое лиць использущие (намереважцеся использователь) ПО для собственных (производственных) нука. Система регистрации легальных пользователей ПО. Конечный Пользователь возмонисть и спользователи ПО по назачениеми регистрации легальных которая предоставляет Конечных Пользователь с возмоность коспользования ПО по назачениеми регистрации деятельных ситеме регистрации.
 Права на ПО В соответствии с настоящим соглашением Вам предоставляется право (неисключительная лицензия) на использование ПО без права копирования.
3. Право свободного использования экземпляра ПО Конечный пользователь, правомерно владежций программно-аппаратным комплексом VIPNet Coordinator HN 4 и согласившийся с условиями настоящего соглашения, вправе использовать ПО на территории Российской Федерации способами, указанными в п. 2, в течение срока действия исключительного права.
 Ограничения Конечный пользователь обязан не нарушать исключительных и иных законных прав Правообладателя на ПО. Сомечный пользователь не вправе передавать третьим лицам ПО и права на него. Конечный пользователь не вправе передавать дизассемблирование (переводить объектный код в исходный), деконплияции, доработку и/лим нодимикацию ПО и совершать другие действия, нарушающие права Правообладателя или
<pre>C Yes > < No ></pre>

ViPNet Key Setup	
Welcome to the ViPNet Coordinator VA 4.3.3–4088! You must install keys or restore saved configuration Would you like to start installing keys or restoring configuration?	
(Press [Next] to start unpacking of the keys)	
<pre></pre>	

Рисунок 8

Please select a continent or	ocean.	1 Africa 2 Americas 3 Antarctica 4 Arctic Ocean 5 Asia 6 Atlantic Ocean 7 Australia 5 Europe 9 Indian Ocean 10 Pacific Ocean 11 UTC	
	< Next >	< Back >	<cance1></cance1>

Рисунок 9

ViPNet Key setup	
Please select a country.	
5	Belarus
6	Belgium
7	Bosnia & Herzegovina
8	Britain (UK)
9	Bulgaria
10	Czech Republic
12	Denmark
13	Estonia
14	Finland
15	France
16	Germany
17	Gibraltar
18	Greece
19	Guernsey
20	Hungary
21	Ineland Tala of Man
22	Isie of han
24	Jerseu
25	Latvia
26	Liechtenstein
27	Lithuania
28	Luxembourg
29	Macedonia
30	Malta
31	Moldova
32	Monaco
33	Montenegro
04	Netheridius
35	Poland
37	Portugal
38	Romania
39	Russia
40	San Marino
+(+)	81%
<pre>/ Nevt N</pre>	(Back) (Cancel)
	Y DURINY Y YOUNDETY

Рисунок 10



Рисунок 11



Рисунок 12

Очень важно, что бы на координаторе были правильно настроены дата и время.

ViPNet Key Setup	
Select current date	
Month Year	
July 2021	
Sun Mon Tue Wed Thu Fri Sat	
27 1 2 3 28 4 5 6 7 8 9 10 29 11 12 13 14 15 16 17	
30 18 19 20 21 22 23 24 31 25 26 27 28 29 30 31	
<pre>< Next > < Back > <cancel></cancel></pre>	

ViPNet Key Setup			
Select current time			
		10 : 3 <u>6</u> : 42	
	< Next >	< Back >	<cancel></cancel>

Рисунок 14



Рисунок 15

Если все до этого момента было сделано верно, то система попросит Вас вставить usb-flash носитель, на котором хранится *.dst файл.

<u> </u>	iPNet Key Setup
	Insert USB storage device with DST or VBE file and press [Next]
	<pre></pre>

Рисунок 16

ViPNet Key Setup		
Discourse in the second line way and been		1
Please wait, mounting USB storage device and look	ing for USI/VBE files	
	08	
	20 X	
	0%	
	0%	
	0%	
	08	
	08	
	08	
	08	
	08	
	08	
	08	
	03	
	03	

Рисунок 17

Если usb-flash был правильно отформатирован, работает исправно и на нем имеется *.dst файл, то система попросит Вас его выбрать. Выберите соответствующий, а скорее всего единственный файл.

/iPNet Key Setup			
Found several DST and/or VBE files Please choose one DST or VBE file			
	/usb/abn_0002.dst /usb/abn_0003.dst /usb/abn_0004.dst	10E9000B Coordinator 2 10E9000C Coordinator 3 10E9000D Coordinator 4	MOBILE
< Nex	t >	< Back >	<cancel></cancel>

Рисунок 18

После выбора *.dst, система запросит ввести пароль. Данный пароль хранится в *.xps файле, который идет в комплекте с *.dst. Если данного файла нет или он был утерян – обратитесь к Администратору сети.

Step 8 – Unpacking DST file			
Enter password for selected USI file			
< Next >	< Back >	<cancel></cancel>	

Рисунок 19

После успешного ввода пароля, система может перезагрузиться. После успешного запуска настройка координатора продолжится.

В координаторе может быть несколько портов. В зависимости от модели, их расположение и количество может различаться. В данной инструкции будет использоваться настройка для работы координатора «в разрез». Для реализации данного варианта достаточно настроить 1 (один) сетевой интерфейс(порт). Примерный вариант данной схемы проиллюстрирован на Рисунок 20.

Однако, согласно требованиям регулятора, Вам необходим сертифицированный межсетевой экран. Координатор является сертифицированным межсетевым экраном, но для выполнения требования, он должен быть установлен в разрыв и иметь два настроенных интерфейса – один на вход и второй на выход. К сожалению, мы не можем полностью проинструктировать Вас по этому вопросу, так как многое упирается в настройки вашей локальной сети и на ваше владение предметом.





В данной инструкции будет настроен сетевой интерфейс eth0. Вы можете настраивать любой удобный для себя сетевой интерфейс. На Рисунок 21 сетевой интерфейс eth0 выбирается

активным, следовательно все другие будут неактивны. Выбор осуществляется клавишей «Пробел».

ViPNet Key Setup		
UP/DOWN settings for interface eth0		
	(*) UP Activate interface on boot () DOWN Don't activate interface on	boot
l		
Next :	< Back >	<cancel></cancel>

ViPNet Key Setup		
Settings for interface eth0		
	() DHCP (*) <mark>StaticIP</mark>	Get IP-address automatically on boot (via DHCP) Set static IP-address
	K Next >	< Back >

Рисунок 22

На данном шаге (Рисунок 23) указывается IP-адрес координатора и его маска. Настраивать Вы вольны в соответствии со своей сеткой. Адрес на скриншоте указан для примера.

ViPNet Key Setup					
	anthing for athe				1
Static IP-address	settings for ethu				
Interface Name					
IP-address	192.168.0.10				
Netmask	255.255.255.0				
	< Next >	< Back >	<canc< th=""><th>el></th><th></th></canc<>	el>	

Рисунок 23

Как и говорилось ранее, остальные интерфейсы отключаются.

Vi	PNet Key	y Setup									
	UP/DOW	N settings	for in	terface e	eth1]
					((*) UP Down	Activate inte Don't activat	rface on boot e interface o	t on boot		
	L										
				K	Next >		< Back >		<cancel></cancel>		

Рисунок 24

На Рисунок 25 указывается маршрут по умолчанию. Здесь следует вписать адрес Вашего роутер, который подключен к координатору.

ViPNet Key Setup				
				1
Enter IP-address of the def	ault gateway			_
IP-address 192.168.0.1				
L				
				-
	< Next >	< Back >	<cancel></cancel>	

Рисунок 25

ViF	Net Key Setup
	Enable/Disable DNS server mode
	() ON Enable starting the DNS server at boot
	<pre></pre>

Рисунок 26

ViPNet Key Setup				
Enable/Disable NTP server mode				
	() ON Enable st (*) <mark>OFF</mark> Disable s	arting the NTP server at tarting the NTP server a	t boot <mark>at boot</mark>	
	nut N		(Papag 1)	
	<u>xt 2</u>	< DALK >	(cancer)	

Рисунок 27

Имя координатора должно соответствовать его физическому расположению и принадлежности к той или иной медицинской организации, а так же примерно совпадать с его именем в ЦУС (данное имя можно уточнить у Администратора сети) или посмотреть на название папки с *.dst или "имя".xps. Если имя в ЦУС не совпадает с физическим местоположением координатора, то сообщите об этом Администратору сети (например координатор переехал из одного филиала в другой).

ViPNet Key Setup							
Enter hostname Or press [Next]	to leave default	: value. Only	latin letters,	digits and '-	' symbols are	allowed (2–6	3 symbols)
GKB-10-stacion	ar						
	K	Next >	< Bac	< >	<cancel></cancel>		

Рисунок 28

ViPNet	Key Setup					
The Do	current virtual IP you want to specify	address range is: custom virtual IP	11.0.0.1/ address r	′8 °ange?		
			() Yes (*) NO	Set custom virtual : Leave the default s	IP range <mark>etting</mark>	
		< <u>N</u> ext		< Back >	<cancel></cancel>	

Рисунок 29

o you w	ant t	o probe	VPN-con	nection	with s	ome host	: in orde	r to ver	ify the	configur	ation yo	bu've ju	st made	?
				< Yes	>		< Ba	sk >		< N	0 >			

<u>V.</u>	iPNet Key Setup	
	Do you want to start VPN services before leaving the installation wizard?]
		-
	C Yes > C Back > C NU >	

Рисунок 31

Finish – начинается перезагрузка.

ViPNet Key Setup				
Satur wizard is successfully completed				
setup wizaru is successiulig completeu.				
C Einich N	,	Pock		(Pup Command challs
	<	Dauk	,	(Kun commanu Sherr)

Рисунок 32

После перезагрузки системы, следует настроить конфигурационный файл службы VPN. Для этого необходимо войти в систему с повышенными правами.

Login	user
Password	«в .xps файле»

Product: ViPNet Coordinator VA Platform: VA VMWARE License: HM-VA Software version: 4.3.3-4088 (C) JSC InfoTeCS, 2020; website: www.infotecs.ru, email: soft@infotecs.ru; phone (Russia): 8 800 250-0-260, phone (Moscow): +7 4 95 737-61-92 GKB-10-stacionar login: user Password: Last login: Thu Jul 22 10:29:34 +05 2021 on tty1 Loading command shell, please wait... Starting the command line interface of Platform: VA VMWARE GKB-10-stacionar> enable Type the administrator password: GKB-10-stacionar# _

Рисунок 33

Затем проверяем, правильно ли были настроены сетевые интерфейсы. Обращаем внимание на выделенные места. Красным выделен интерфейс, который и планировалось настроить. Сверьте планируемые настройки с фактическими. Синим выделен интерфейс, который не планировалось включать. Для скроллинга используйте комбинацию клавиш shift + pageUp / shift + pageDown.



Рисунок 34

Если интерфейсы настроены верно, то можно приступать к настройке конфигурационного файла iplir.conf. Для начала необходимо остановить службу iplir командой *iplir stop*.



Рисунок 35

Затем открыть конфигурационный файл командой iplir config.



Рисунок 36

Затем необходимо найти в файле секцию [dynamic] (лучше начинать с конца).

	GNU	nano	2.3.6		
[dynar	nic]			
d	ynam:	ic_pro	oxy= ofi	f	
f	orwar	rd_id=	= 0x0000	00000	
а	lways	s_use_	_server:	= off	
t	imeou	ut= 25	5		
p	ort_a	auto_d	change=	off	

Рисунок 37

Отредактировать в ней следующие параметры:

- dynamic_proxy= on
- forward ID= 0x0c1c2860

GNU nano 2.3.6
[dynamic]
dynamic_proxy= on
forward_id= 0x0c1c2860
always_use_server= off
timeout= 25
port_auto_change= off

Рисунок 38

После чего сохранить изменения. Для этого комбинацией клавиш *ctrl+x* необходимо выйти из редактора и согласиться с изменениями не изменяя название файла (Enter).

Save	modified	buffer	(ANSWERING	"No"	WILL	DESTROY	CHANGES)	?
Y Ye	s	_						
N NC)	îC Ca	ancel					
Рисунок 39								
	Cile N	+-	lleiter (tem	1.1.1 mm		aa /ialia	aanf	
	AC OFT	ame to	write: /tmp	/vipn	ietzus	ervipiir	.cont_	
	G Get	нетр						
		CGT						

После необходимо запустить службу iplir командой *iplir start* и перезагрузить координатор командой *machine reboot*.



Возможные проблемы (FAQ):

1. Возможна неверная настройка сети.

Попробуйте проверить сетевую доступность устройства командами:

- inet ping <ip-address шлюза>
- inet ping 8.8.8.8

Если выполнение данных команд не увенчалось успехом — значит проблема в локальной настройке. Тут Вы сами себе хозяева, помочь не сможем.

2. Возможно неверно настроен туннель на координаторе или статический маршрут Проверьте, есть ли доступ с координатора до ПроМед командами:

- *iplir ping 0x0c1c2860* (если команда считается неправильной введите iplir start и повторите)
- iplir ping 10.62.15.30

Если команды завершились успешно — значит проблема или в туннеле или в маршруте — подсказа по настройке маршрута есть на *сайте миац-рб.рф* → Деятельность → Информационная безопасность.

3. Проверка настроек туннеля

Введите команду *iplir show config*. В первой секции [id] будут указаны туннели, которые заданы Вашему координатору. Для их смены необходимо написать заявку на почту <u>oib@doctorrb.ru</u> и указать в нем название координатора и требуемое адресное пространство для туннелирования.

4. Проверка настроек конфигурационного файла

Введите команду iplir show config и в случае, когда корд стоит сбоку (один активный сетевой интерфейс) проверьте следующие параметры:

- В собственной секции [id] (самая первая где ваши туннели): о параметр usefirewall установите в значение on;
- В секции [dynamic]: о параметр dynamic_proxy установите в значение on;
- в параметре forward_id = 0x0c1c2860;
- **5.** Для предоставление удаленного доступа по ssh firewall local add src (айпишник с которого будешь заходить) dst (айпишник корда) service @SSH pass
- 6.
 Telegram чат для решения и обсуждения проблем

 https://t.me/+QSyMCxV085szMjVi

