

НИИ ТГУ «Национальный исследовательский Томский государственный университет»

Тема проекта: Администрирование СКЗИ «Vipnet Coordinator 1000 HW

Подготовил: Марков Д.К.

Руководитель проекта: Тренькаев В.
Н.

Дата: 03.11.2021

Администрирование средств защиты информации в КГБУЗ «Назаровская районная больница»

Имеющиеся в эксплуатации средства защиты:

1. Программно-аппаратный комплекс (криптошлюз и межсетевой экран Vipnet Coordinator HW1000 (производитель Аквариус), программные комплексы Vipnet Client
2. Комплексная антивирусная защита корпоративной сети – Dr.Web Enterprise Security Suite (Центр управления)
3. Средства администрирования на базе ОС Windows с правилами делегирования полномочий пользователей

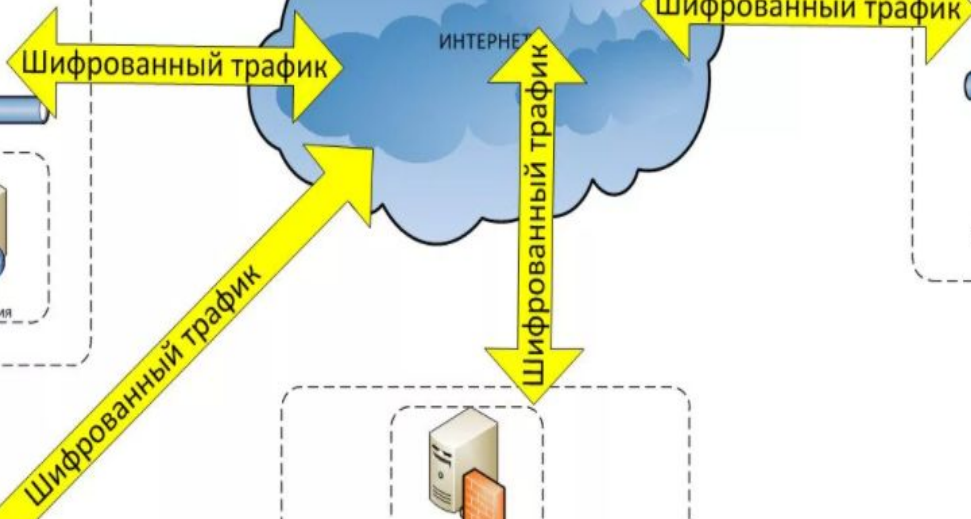
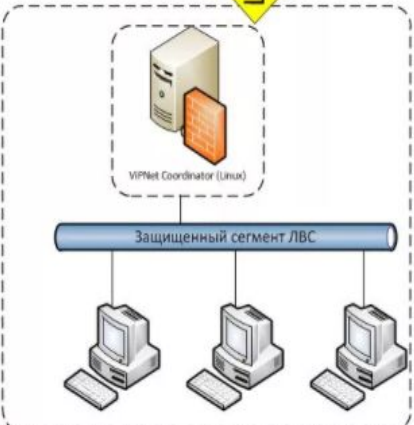
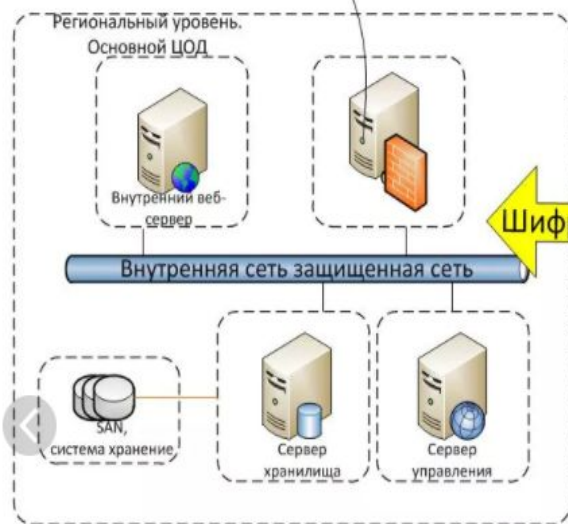
Региональный сегмент государственной информационной системы здравоохранения Красноярского края

Участники:

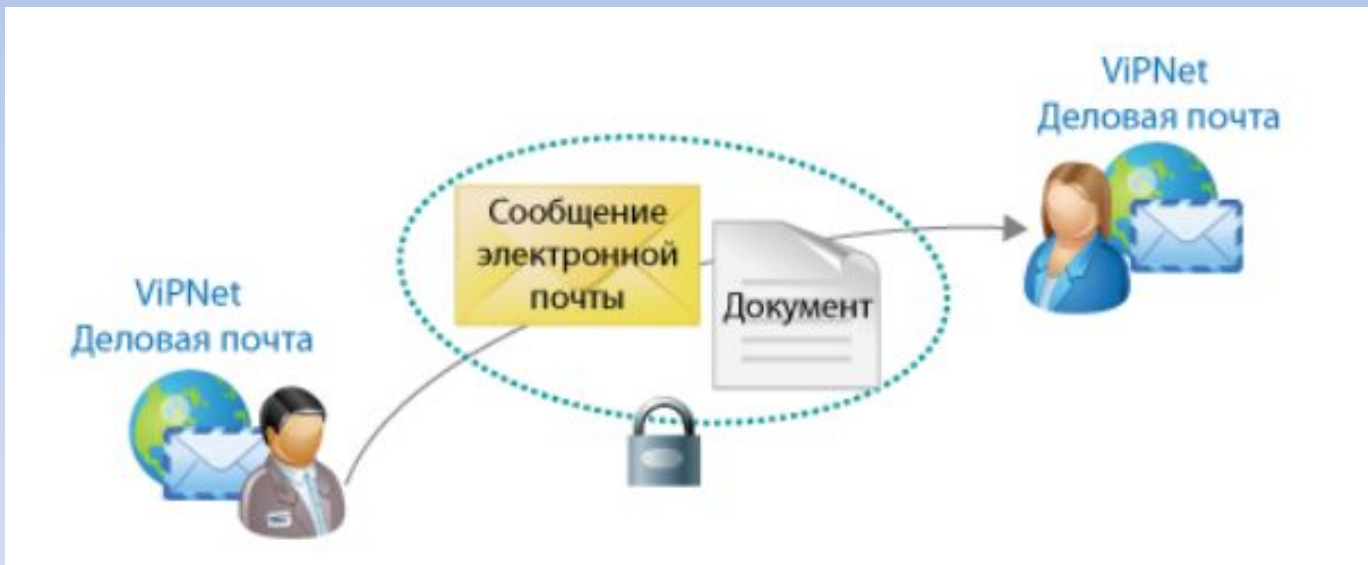
- Медицинские организации в системе ОМС
- Страховые медицинские организации
- Территориальный фонд ОМС Красноярского края
- Краевой медицинский информационно-аналитический центр

Защищенная сеть регионального сегмента информационной системы

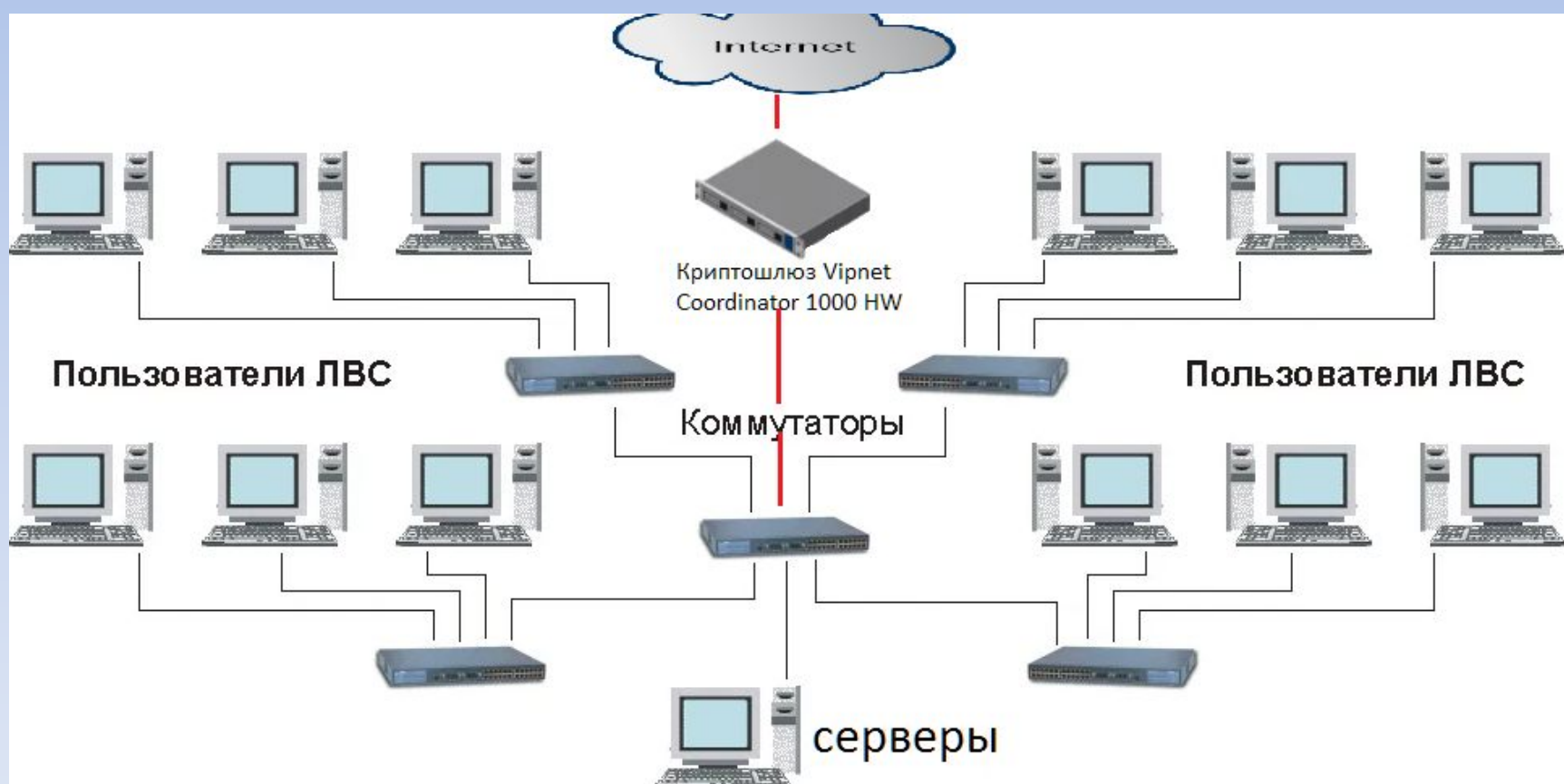
Комплекс программного обеспечения VIPNet CUSTOM, предназначенный для организации и координации распределенной VPN сети



Защищенный электронный документооборот между участниками сегмента



Примерная схема организации ЛВС внутри КГБУЗ «Назаровская РБ»



Сценарии использования VipNet Coordinator 1000 HW

- Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site).
- Защита магистральных каналов, соединяющих ЦОДы между собой.
- Защита беспроводных сетей связи 3G и Wi-Fi.
- Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
- Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ).
- Защищенный доступ удаленных и мобильных пользователей.
- Взаимодействие с сетями VipNet других организаций.

Преимущества

- Организация VPN на сетевом (L3) и канальном уровне (L2)* в одном устройстве.
- Кластер горячего резервирования.
- Работа в необслуживаемом режиме.
- Централизованное и удаленное управление (SSH, WebUI).
- Поддержка работы в современных мультисервисных сетях связи без ограничений по совместимости:
 - со службами DHCP, WINS, DNS;
 - с динамическим преобразованием адресов (NAT, PAT);
 - с использованием мультимедийных протоколов (SIP, H323, SCCP и другие)

Сертификация:

Сертификат соответствия ФСБ России

Сертификат соответствия ФСТЭК России

Сертификат соответствия Минкомсвязи России

+ ряд патентов

Демонстрация оболочки (Общее меню координатора)

ViPNet Coordinator HW1000

Меню координатора
HW1000.jpg
Тип: Файл "JPG"
Размер: 103 КБ
Разрешение: 884 x 722 пкс



VPN



Межсетевой
экран



Прикладные
сервисы



Сетевые
настройки



Системные
настройки



Мониторинг

Демонстрация оболочки (внешний сетевой интерфейс)

VIPNet Coordinator HW1000

← Сетевые интерфейсы Маршрутизация

- Ethernet (eth0)
- Ethernet (eth1)
- Ethernet (eth2)
- Ethernet (eth3)

Обновить

Интерфейс eth0 Включен

Соединение:	Сетевой кабель подключен
MAC-адрес:	68:05:ca:06:d2:ec
Скорость:	1000Mb/s
Режим передачи данных:	Дуплекс
Класс:	Access
Настройка подключения:	Вручную
IP-адрес:	
Маска подсети:	255.255.255.224

Дополнительные IP-адреса

IP-адрес	Маска подсети
Дополнительные IP-адреса не заданы	

Демонстрация оболочки (внутренний сетевой интерфейс)

VIPNet Coordinator HW1000

← Сетевые интерфейсы Маршрутизация

- Ethernet (eth0)
- Ethernet (eth1)
- Ethernet (eth2)
- Ethernet (eth3)

Обновить

Интерфейс eth1 Включен

Соединение:	Сетевой кабель подключен
MAC-адрес:	68:05:ca:06:d2:ed
Скорость:	100Mb/s
Режим передачи данных:	Дуплекс
Класс:	Access
Настройка подключения:	Вручную
IP-адрес:	10.48.0.1
Маска подсети:	255.255.254.0

Дополнительные IP-адреса

IP-адрес	Маска подсети
Дополнительные IP-адреса не заданы	

Демонстрация оболочки (Общая статистика)



Выберите

Наименование пакета	Входящие		Исходящие		Блокированы
	Получены	Блокированы	Получены	Блокированы	
Открытые	3089293981	35810324	3055785432	761	
Зашифрованные	2046331	11975	48213031	52458	
Широковещательные	3353357	48673	0	0	
Широковещательные зашифрованные	12071	0	18230	3930	

Общая статистика по пакетам.jpg
Тип: Файл "JPG"
Размер: 101 КБ
Разрешение: 1919 x 839 пкс

Демонстрация оболочки (статистика и мониторинг пакетов)

VPNNet Coordinator HW1000



Войти как администратор Выйти

← Состояние системы Статистика и журналы

Журнал регистрации IP-пакетов

Статистика

Результаты за последний час с 03.11.2021 09:16



Просмотр IP-пакета

Обновить

	Конец интервала	Источник	Порт источника	Назначение	Порт назначения	Протокол	Количество	Размер	Событие
✓ ←	03.11.2021 10:16	10.48.0.171	7506	134.130.241.22	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50885	155.65.31.244	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.171	7507	133.49.13.70	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.241	61180	43.142.34.230	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.248	61530	16.78.76.75	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50889	90.28.175.109	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50891	145.203.186.197	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50893	125.76.166.206	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50879	222.225.29.154	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.171	7501	170.11.196.210	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.171	7503	42.69.142.106	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.1.208	50728	77.88.21.119	443	6-TCP	1	41	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.171	7505	35.202.44.99	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.4	53944	186.220.67.49	445	6-TCP	1	52	62-Пропущен незашифр...
✓ →	03.11.2021 10:16	104.26.8.169	443	10.48.0.162	62293	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.4	53947	121.9.128.193	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50892	41.234.131.90	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.4	53950	96.93.64.229	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50894	164.206.70.244	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50896	217.151.96.2	445	6-TCP	1	52	62-Пропущен незашифр...

Демонстрация оболочки (критерии поиска пакетов)

Скрыть критерии поиска



Просмотр IP-пакета

Обновить

Признаки IP-пакетов

Сетевой интерфейс:

Тип трафика:

Тип адреса:

Трансляция:

Событие:

Протокол:

Источник

IP-Адрес:

Сетевой узел: [Мой узел](#)

Порт:

искать в обоих направлениях

Назначение

IP-Адрес:

Сетевой узел: [Мой узел](#)

Порт:

Критерии поиска мониторинга пакетов.jpg
Тип: Файл "JPG"
Размер: 184 КБ
Разрешение: 1917 x 827 пкс

Общие

Период регистрации:

Отображать не более: последних записей

Найти

Восстановить значения по умолчанию

	Конец интервала	Источник	Порт источника	Назначение	Порт назначения	Протокол	Количество	Размер	Событие
✓ ←	03.11.2021 10:16	10.48.0.171	7506	134.130.241.22	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.25	50885	155.65.31.244	445	6-TCP	1	52	62-Пропущен незашифр...
✓ ←	03.11.2021 10:16	10.48.0.171	7507	133.49.13.70	445	6-TCP	1	52	62-Пропущен незашифр...

Демонстрация оболочки (Фильтры защищенной сети)

VPNNet Coordinator HW1000

← Сетевые фильтры NAT Группы объектов Прокси-сервер

Фильтры защищенной сети | Фильтры туннелируемых узлов | Локальные фильтры открытой сети | Транзитные фильтры открытой сети

Просмотр

Имя фильтра	Статус	Действие	Протоколы	Источники	Назначения
Фильтры политики безопасности из Policy Manager					
8080_22_Allow		Разрешает	TCP:to 8080, TCP:to 22		
8080_22_Drop		Блокирует	TCP:to 8080, TCP:to 22	Все	Мой узел
Настраиваемые фильтры					
Broadcast Converted Rule		Разрешает	UDP:from 137 to 137, UDP:from 138 to 138, UDP:from 67 to 68, UDP:from 2046 to 2046, 2050 to 2050		Широковещательные адреса
Broadcast Converted Rule		Разрешает	UDP:from 137 to 137, UDP:from 138 to 138, UDP:from 67 to 68, UDP:from 68 to 67, UDP:from 0-65535 to 2046, UDP:from 0-65535 to 2048, UDP:from 0-65535 to 2050	Другие узлы	Широковещательные адреса
Broadcast Converted Rule		Блокирует	Все объекты	Все	Широковещательные адреса
Main Converted Rule		Разрешает	Все объекты	Все	Все
Фильтры по умолчанию					
Прочий трафик		Блокирует	Все объекты	Все	Все

Фильтры защищенной сети.jpg
Тип: Файл "JPG"
Размер: 158 КБ
Разрешение: 1649 x 829 пкс