Внимание:

* Схемы внутри документа можно открыть с помощью Visio. Для этого необходимо нажать правой кнопкой мыши на схеме и выбрать пункт «Объект Visio> Открыть».
* Для отрисовки каналов связи между устройствами используйте информацию из конфигурационных файлов (show cdp neighbors, description на интерфейсах), а также читайте информацию в примечаниях.
* При разработке схем используйте фигуры Visio из шаблонов.
* Обратите внимание, что устройства ViPNet Coordinator выполняют роль межсетевых экранов и шлюзов криптографической защиты. Соответственно, необходимо использовать правильную фигуру из шаблона.
* Конфигурационные файлы приложены в конце файла

**Задание:**

1. Разработать структурную схему сети.

На схеме необходимо:

* Указать здания и помещения (в виде границ), в которых расположено сетевое оборудования
* Отобразить сетевые устройства (коммутаторы, маршрутизаторы), с указанием модели устройства и имени (для каждого устройств) в рамках указанных помещений
* Отобразить сетевые средства безопасности с указанием модели устройства и имени (для каждого устройства)
* Отобразить физические каналы связи, организуемые между устройствами, с указанием используемых интерфейсов с обеих сторон (тип интерфейса, номер интерфейса).

**Примечание:** проектируемые линии связи отображаются жирной линией, используемые существующие линии связи отображаются тонкой линией.

* Отобразить каналообразующее оборудование (например: медиаконвертеры), при его наличии
* Отобразить подключаемых провайдеров Интернет
* указать условные графические обозначения, используемые на схеме

1. Разработать логическую схему сети:

На схеме необходимо:

* Отобразить проектируемые сегменты сети
* Отобразить устройства, терминирующие на себе сегменты сети (устройства, являющиеся шлюзами в данных подсетях) с указанием модели устройства и его имени
* указать ip-адреса и интерфейсы со стороны устройств в рамках каждого сегмента
* указать условные графические обозначения, используемые на схеме

**Исходные данные:**

1. Перечень используемого сетевого оборудования, каналообразующего оборудования и сетевых средств защиты

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Но- мер | Наименование | Сетевое имя | Расположение | Примечание |
|  | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S (2 шт.) | BLG-KDP-FL.2-SW-CORE | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Коммутатор доступа Cisco WS-C2960RX-48TS-L | BLG-KDP-Fl.3-SW-ACC | Здание КДП, 3 этаж, каб. 308 | проектируемое |
|  | Стек коммутаторов периметра Cisco WS-C2960RX-24TS-L (2 шт.) | BLG-KDP-Fl.2-SW-EXT | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Коммутатор сети видеонаблюдения | Отсутствует | Здание КДП, 3 этаж, каб. 317 | существующее |
|  | Маршрутизатор периметра Cisco ISR4221 | BLG-KDP-Fl.2-RT-EXT-1 | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Маршрутизатор периметра Cisco ISR4221 | BLG-KDP-Fl.2-RT-EXT-2 | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Основной шлюз кластера ViPNet Coordinator HW1000 | BLG-KDP-Fl.2-FW-VPN-1 | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Резервный шлюз кластера ViPNet Coordinator HW1000 | BLG-KDP-Fl.2-FW-VPN-2 | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Система обнаружения вторжений ViPNet IDS 1000 | BLG-KDP-Fl.2-IDS | Здание КДП, 2 этаж, каб. 216 | проектируемое |
|  | Медиаконвертер GL-GU-SFP-v2 | Отсутствует | Здание КДП, 2 этаж, каб. 216 | Существующее (используется для организации канала связи между коммутатором ядра и коммутатором доступа, расположенным в административном здании). Канал связи от медиаконвертера до коммутатора в здании Здание КДП – проектируемый медный.  Канал связи до другого медиаконвретера – существующий оптический (одномод) |
|  | Медиаконвертер GL-GU-SFP-v2 | Отсутствует | Административное здание, 1 этаж, каб. 7 | Существующее (используется для организации канала связи между коммутатором ядра и коммутатором доступа.  Подключение в сторону другого медиаконвертера по существующей одномодовой оптическй линии связи.  Подключение к коммутатору в административном здании по сущетсвующей медной линии связи |
|  | Коммутатор доступа Cisco WS-C2960X-48TD-L | BLG-ADM-Fl.1-SW-ACC | Административное здание, 1 этаж, каб. 7 | Существующее |

1. Перечень сетевых сегментов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Номер VLAN** | **Наименование сегмента** | **IP-подсеть** | **Точка терминации/шлюз** | **Назначение сегмента** |
| 110 | Management | 10.27.121.0/25 | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S | Сегмент управления сетевым и серверным оборудованием |
| 111 | SZI\_Management | 10.27.121.128/26 | Кластер ViPNet Coordinator HW1000 | Сегмент управления СЗИ |
| 120 | Users\_&\_Printers | 10.27.122.0/24 | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S | Сегмент пользователей и принтеров |
| 121 | Users\_ISPDN | 10.27.123.0/26 | Кластер ViPNet Coordinator HW1000 | Сегмент пользователей ИСПДн |
| 124 | VKS | 10.27.129.0/27 | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S | Сегмент ВКС |
| 126 | Video | 10.27.129.32/27 | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S | Сегмент видеонаблюдения |
| 140 | Servers | 10.27.124.0/27 | Стек коммутаторов уровня ядра Cisco WS-C3650-24TS-S | Сегмент серверов |
| 170 | DMZ | 10.27.127.0/27 | Кластер ViPNet Coordinator HW1000 | Сегмент ДМЗ |
| 500 | LAN\_IN | 10.27.120.0/28 | Кластер ViPNet Coordinator HW1000 | Транзитный сегмент (для организации логического соединения между внутренними интерфейсами шлюзов VipNet Coordinator HW1000 и стеком коммутаторов ядра) |
| 501 | LAN\_OUT | 10.27.120.16/28 | Кластер ViPNet Coordinator HW1000 | Транзитный сегмент (для организации логического соединения между внешними интерфейсами шлюзов VipNet Coordinator HW1000 и внутренними интерфейсами маршрутизаторов периметра |
| 700 | ISP1\_ Rostelekom | 89.109.153.184/29 | Маршрутизатор Cisco ISR4221 (BLG-KDP-Fl.2-RT-EXT-1) | Сегмент подключения провайдера ПАО «Ростелеком» |
| 701 | ISP2\_ Megafon | 31.173.239.120/29 | Маршрутизатор Cisco ISR4221 (BLG-KDP-Fl.2-RT-EXT-2) | Сегмент подключения провайдера ПАО «Мегафон» |

1. Выгрузки конфигурационных файлов и результатов выполнения диагностических команд (предоставлены в отдельных текстовых файлах).
2. Настройки кластера ПАК VipNet Coordinator HW 1000

Таблица – Адреса интерфейсов ПАК ViPNet Coordinator

| **Название интерфейса** | **Active IP**  **BLG-KDP-Fl.2-FW-VPN** | **Passive IP**  **BLG-KDP-Fl.2-FW-VPN-1** | **Passive IP**  **BLG-KDP-Fl.2-FW-VPN-2** |
| --- | --- | --- | --- |
| eth0.111 | 10.27.121.129/26 | 10.27.121.130/26 | 10.27.121.131/26 |
| eth0.121 | 10.27.123.1/26 | 10.27.123.2/26 | 10.27.123.3/26 |
| eth0.500 | 10.27.120.2/28 | 10.27.120.3/28 | 10.27.120.4/28 |
| eth1 | - | 10.27.121.193/30 | 10.27.121.194/30 |
| eth2 | 10.27.127.1/27 | 10.27.127.2/27 | 10.27.127.3/27 |
| eth3 | 10.27.120.20/28 | 10.27.120.21/28 | 10.27.120.22/28 |

1. Настройка ViPNet IDS

Таблица – Адреса интерфейсов ViPNet IDS

|  |  |
| --- | --- |
| **Интерфейсы** | **ViPNet IDS** |
| Eth0 | 10.27.121.132 |
| Eth1 | Интерфейс, прослушивающий трафик |
| Eth2 | Не используется |
| Eth3 | Не используется |

**Пример проектируемой структурной схемы:**



**Пример проектируемой логической схемы:**

1. **Пример №1:**



**Примечание:** на данной схеме не хватает информации относительно имён устройств, логических интерфейсов

**Пример №2:**



Конфигурационные файлы:

