ПРОФЕССИОНАЛЬНОЕ КОНКУРСНОЕ ЗАДАНИЕ
ИНВАРИАНТНАЯ ЧАСТЬ ЗАДАНИЙ

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) одного из интеграторов DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и развернуть DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом Active Directory), с которым необходимо будет осуществить интеграцию DLP-системы. До действий по интеграции и установке компонент системы необходимо подготовить доменных пользователей.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM).

Необходимо развернуть компоненты уровня сети (network) и хоста (endpoint).

Вам необходимо установить и настроить компоненты DLP-системы в соответствии с выданным заданием. Все необходимые файлы размещены на рабочем столе хостовой машины в папке Олимпиада.

Необходимо использовать следующие виртуальные машины:

- AD2 (контроллер домена demo.lab)
- IWTM (Node+DB) (необходимо настроить)
- IWDM (Node+Server) (Windows Server для IWDM)
- w10-cli1 (ПК Windows первого нарушителя)

Сетевые настройки виртуальных машин:

машина	Настроенные параметры IP	Установленное ПО	пользователь
AD2	Eth1 192.168.131.10 255.255.255.0 Eth2 Параметры по DHCP	ОС Windows Server 2019 Настроенный домен demo.lab, с настроенными службами DHCP, DNS, маршрутизация и удаленный доступ	Администратор Пароль Admin2025
IWTM	Eth1 192.168.131.20 255.255.255.0 Шлюз 192.168.131.10	ОС Centos 7 IWTM 6.11 (пользователь officer, пароль xxXX1234)	Root Пароль Admin2022
IWDM	Eth1 192.168.131.30 255.255.255.0 Шлюз 192.168.131.10	ОС Windows Server 2019 Машина введена в домен demo.lab БД Postgres, ПО IWDM (пользователь officer, пароль xxXX1234)	Администратор Пароль Admin2025

Net1-Open	Eth1 Не настроен	ОС Windows 10	Student Пароль 111111
Net3-Open	Eth1 Не настроен	ОС Windows 10	Student Пароль 111111

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах (https://kb.infowatch.com/).

Задание 1: Подготовка Active Directory

Для дальнейших работ рекомендуется создать подразделение организации (Organization Unit) под названием «Olimp», добавить в него новые каталоги пользователей и компьютеров (Users и Computers). В каталог Users рекомендуется добавить следующих пользователей и задать для всех пользователей пароль xxXX1234:

— admin-dm (права доменного администратора), пользователь для машины IWDM и консоли IWDM

— admin-db (права доменного администратора, для консоли IWDM)

— useroffice1 (1 машина W10, права пользователя домена, W10-cli)

— ldapuser (права пользователя домена), пользователь для осуществления LDAP-синхронизации

— tmofficer (права пользователя домена), пользователь для входа в веб-консоль.

Рекомендуется после ввода в домен, компьютеры необходимо переносить в ранее созданный каталог Computers (внутри OU «Olimp»)

В соответствии с политикой компании для обеспечения безопасности компьютеров брандмауэр должен быть активен. Для установки компонентов системы необходимо настроить правила брандмауэра с помощью групповых политик домена. Зафиксировать скриншотами и вставить в этот файл с заданием.

Настройте LDAP-синхронизацию для IWTM с помощью пользователя ldapuser. (Зафиксировать скриншотами)

Для работы с консолью IWTM используйте доменного пользователя tmofficer (задать все встроенные роли (officer и administrator) и все области видимости). Зафиксировать скриншотами.

Уже развернуты, но не настроены следующие компоненты InfoWatch Device Monitor (IWDM): БД PostgreSQL, основной Сервер IWDM и Консоль управления.

Агентов IWDM на машины «нарушителей требуется установить Вам.

Технологии агентского мониторинга

Зафиксируйте все этапы настройки, создания и выполнения (срабатывание, где возможно) всех групповых политик скриншотами и вставьте в этот документ после соответствующего задания.

Настройка IWDM. Используйте для входа в консоль IWDM доменного пользователя admin-dm в т. ч. для входа в консоль без пароля (галочкой).

Проверить работоспособность, зафиксировать настройку и выполнение скриншотом запущенной консоли.

Необходимо создать и выполнить задачу создания пароля для деинсталляции для машин, к которым это применимо. Пароль: xxXX1234

Необходимо создать политику «Отдел 1», применить ее на группу компьютеров, в которую входит Net1-Open.

Правило 1.

Необходимо запретить создание снимков экрана в табличных процессорах (OpenOffice Calc) и калькуляторе для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Правило 4

Необходимо поставить на контроль буфер обмена в текстовых процессорах (Wordpad).

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Правило 5

На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность попыткой копирования текста из сеанса RDP и зафиксировать выполнение скриншотом. Для работы RDP может потребоваться дополнительная настройка.

Правило 6

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера Chrome путем создания снимков экрана каждые 60 секунд или при переходе в другое окно.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в консоли IWTM.

Подтвердить выполнение задания скриншотами свойств пользователя со снимками экрана в IWTM.

Правило 7

Создать политику по блокировке копирования исполняемых exe-файлов на USB накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 8

Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mov, *.mp4) в общих папках компании.

Контролировать файлы больше 10 Мбайт и меньше 1000 Мбайт. (1 Мбайт = 1024 Кбайт) средствами IWDM.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 9

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать облачные хранилища dropbox и google drive, разрешить только скачивание с Yandex disk, остальные сервисы оставить открытыми.

Проверить работоспособность запрета.

Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления ТМ: категориями и терминами, технологиями, объектами защиты и т. п.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании

При правильной настройке политики InfoWatch Traffic Monitor должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться. Должны быть выявлены все инциденты безопасности.

Необходимо пользоваться объектами защиты.

Необходимо настроить доступ к системе пользователя auditor с правами просмотра отчетов и созданных политик, без возможности что-то изменять. Пароль задать xxXX1234.

Создайте список веб-ресурсов и назовите его «Сайты партнеров». Туда необходимо включить следующие веб-ресурсы: kb.infowatch.com, worldskills.ru, infotecs.ru

Для правильной работы системы необходимо настроить периметр компании:

Домен: demo.lab.

Список веб ресурсов: Сайты партнеров

Группа персон: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Политика 1

В связи с санкциями и растущим курсом валют, компания ООО Demo Lab решила сэкономить и закупила программное обеспечение на компьютеры сотрудников у китайских партнеров. Проконсультировавшись с отделом безопасности, руководство компании выяснило, что отдел закупок пошел на большие риски – китайское ПО собирает огромное количество аналитических сведений о машинах, на которых оно работает.

Дабы предотвратить какие-либо утечки, необходимо заблокировать доступ к поддоменам, собирающим аналитику: «capital.tencent.com», «yanekral.tencent.com», «blm.tencent.com»; запретить отправку данных за пределы компании, содержащую информацию о «железе» — упоминания AMD, Intel, Байкал, Эльбрус, МСТ в любом регистре.

Проверку проводить при отправке на почтовые домены.

Вердикт: Заблокировать ×

Уровень нарушения: высокий •

Тег: Политика 1

Политика 2

В последнее время бюджет компании стал резко падать. Подозрения пали на главного бухгалтера, директор подозревает его в проведении денежных средств «мимо кассы». В связи с этим необходимо отслеживать передачу всех номеров и сканов кредитных карт, отправляемых из отдела Бухгалтерии

Вердикт: Заблокировать ×

Уровень нарушения: высокий •

Тег: Политика 2

Политика 3

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «3-4 буквы (латиница, любой регистр) - (знак дефиса) номер груза (с ведущими нулями от 0000 до 1000, исключая следующие номера: 0777 и 0013) . (точка) от 1 до 3 букв (кириллица, верхний регистр) Например: jDhT-0003.Л, kSR-0665.ЪГА, jHy-0920.ЩЗ Не должно быть срабатывания на следующие номера грузов (например:

kdO-0013.ю или jtfd-0777.ШАП). Необходимо контролировать передачу, а также копирование на съемные носители и печать вышеуказанных данных. Проверить работоспособность. Учтите, что особо обобщенные регулярные выражения лучше разделить на несколько текстовых объектов для оптимизации поиска.

Вердикт: Разрешить

Уровень нарушения: средний •

Тег: Политика 3

Политика 4

Необходимо создать политики для отслеживания документов (передача и копирование), содержащих договор компании (договор компании.doc).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненный шаблон, до 25% изменений) – разрешать, уровень низкий, тег «Политика 4.1».

2. Если передается договор компании, в котором присутствует фамилия генерального директора, а также главного бухгалтера – разрешать, уровень средний, тег «Политика 4.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.

3. Если передается договор компании, в котором присутствует фамилия генерального директора, главного бухгалтера, а также стоит печать компании (ООО Повозка) – разрешить, уровень высокий, тег «Политика 4.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 4.1, Политика 4.2, Технология 4.3 и т. д.)

Вердикт 1: Разрешить

Уровень нарушения 1: низкий •

Тег 1: Политика 4.1

Вердикт 2: Разрешить Ö

Уровень нарушения 2: средний •

Тег 2: Политика 4.2

Вердикт 3: Заблокировать ×

Уровень нарушения 3: высокий •

Тег 3: Политика 4.3

Политика 5

В честь юбилея компании была запущена акция с промокодами на скидку в 70% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов из отдела продаж, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («коды.docx»). Стоит учесть, что сотрудники могут слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах.

Проверить работоспособность на все купоны и на 1-2 купона.

Вердикт: заблокировать ×

Уровень нарушения: средний •

Тег: Политика 5

Политика 6

При переезде в новый просторный офис, компанией ООО Demo Lab был расширен штаб сотрудников – было решено взять несколько десятков выпускников технических вузов на стажировку. Для того, чтобы они работали более эффективно, директор компании предложил отслеживать сообщения, содержащие IP-адреса версии 6. Так как предприимчивые выпускники «в тихую» проводят внутренние соревнования по Counter-Strike разворачивая локальные сервера внутри компании. IP – адреса могут иметь следующие конструкции:

IPv6 – адрес (например 2001:0db8:abf2:29ea:5298:ad71:2ca0:4ff1)

IPv6 – адрес + префикс (например2001:0db8:abf2:29ea:5298:ad71:2ca0:4ff1/32)

Во избежание ложных срабатываний, следует отключить политику после проверки.

Вердикт: Заблокировать ×

Уровень нарушения: высокий •

Тег: Политика 6

Политика 7

Необходимо поставить на мониторинг все файлы сертификатов PKCS#7, так как попытки передачи таких данных несут потенциальную опасность компрометации сервисов компании.

Проверить работоспособность.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: Политика 7

Политика 8

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров отправлять документы, содержащие информацию о СНИЛС, ИНН, паспортных данных (в текстовом и графическом виде) за пределы компании.

Вердикт: заблокировать ×

Уровень нарушения: средний •

Тег: Политика 8

Политика 9

Два месяца назад в компании DemoLab заметили, что сотрудница отдела кадров расходует в три раза больше бумаги, чем прежде, хотя объем работ не был увеличен. Путем наблюдения за сотрудницей было установлено, что она, состоя в совете школьной родительской общественности, регулярно собирает деньги с родителей за печать докладов и рефератов учеников класса, бесплатно распечатывая их в компании.

Необходимо создать политику безопасности, которая будет включать слова (с учетом морфологии): «реферат», «доклад», «ученик», «школа», «класс».

Проверку необходимо проверить путем отправки документа на печать и при помощи электронной почты.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: Политика 9

Политика 10

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 5%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5(пяти) популярных на данный момент сериалов при передаче через вебсообщения и почту.

Список: Твин Пикс, Рыцарь дорог, Беспринципные, Уэнсдей, Wednesday.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: Политика 10

Анализ выявленных инцидентов

Задание 1: Сводки

Создайте новые вкладки сводки в разделе «Сводка» под названием «Olimp25» и «Особые сводки Olimp25»

Задание 2: Виджеты

При создании выборок для сводок необходимо помещать их в каталог выборок «Olimp25». Создайте в сводке «Olimp25» 4 виджета:

1. Выборка по событиям краулера за последнюю неделю

2. Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последние 3 дня

3. Статистика по политикам за последние 7 дней

4. Топ нарушителей за последние 3 дня

Задание 3

Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки», отображающий события с уровнем угрозы от низкого до высокого на правила копирования и хранения за последние 7 дней.

Зафиксировать скриншотом конструктора выборки.

Исследование (аудит) организации с целью защиты от угроз информационной безопасности

Вам, как специалисту, поручено разработать концепцию политики защиты данных с целью реализации мер по обеспечению безопасности персональных данных (152-ФЗ, ПП1119, Приказ ФСТЭК России №21 и другие документы). В процессе проведения аудита и формирования политики защиты персональных данных Вы должны решить следующие задачи:

1. В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" определить уровень защищенности персональных данных при их обработке в информационной системе организации. Решение обосновать.
2. В соответствии с Приказом ФСТЭК России N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" определить содержание мер по обеспечению безопасности персональных данных, адаптируя базовый набор мер под требования решения задач обеспечения целостности информационной системы и персональных данных (ОЦЛ).

3.Для реализации мер обеспечения целостности информационной системы и персональных данных необходимо сформировать концепцию политики защиты данных (в соответствии с шаблоном, представленном в приложении), описав:

— используемые технологии анализа,
— объекты защиты,
— списки отправителей/получателей,
— политики защиты данных,
— правила агентского мониторинга.

Концепция политики защиты данных, должна предусматривать:

— выявление фактов неправомерной передачи защищаемой информации из информационной системы через различные типы сетевых соединений, включая сети связи общего пользования и реагирование на них;

— выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и реагирование на них;

— выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию и реагирование на них;

— выявление фактов неправомерного копирования защищаемой информации в прикладное программное обеспечение из буфера обмена и реагирование на них;

— контроль хранения защищаемой информации на серверах и автоматизированных рабочих местах;

— выявление фактов хранения информации на общих сетевых ресурсах (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

Исходные данные

Научно-исследовательская компания «Демо Лаб» (далее - Оператор) занимается контрактной разработкой и продажей перспективных электронных систем в интересах государственных и коммерческих организаций.

Компания обладает значительной клиентской базой, детальной информацией о партнёрах, заказчиках, клиентах за 10 лет работы. Клиентская база (около 2000 клиентов) составляет основу для деятельности по направлению продаж электронных компонент, но не оказывает влияния на направление системных разработок.

С точки зрения кадрового, бухгалтерского и финансового документооборота компания является типовой для Российской федерации.

Сотрудники (300 человек) могут обмениваться информацией посредством Почты/Email, мессенджеров/WhatsApp. Также у ряда сотрудников есть корпоративные сотовые телефоны, через которые также проходит обмен информацией.

ИСПДн Оператора (клиентская часть приложения, реализующая интерфейс пользователя) функционирует на базе АРМ под управлением ОС MS Windows 10 и состоит из следующих программных компонентов:

СУБД Microsoft SQL Server 2019;

— 1С Предприятие: Бухгалтерия (версия 8);

— 1С Зарплата и управление персоналом (версия 8);

— СБиС.

ИСПДн предназначены для автоматизации обработки информации:

— ПДн лиц, которые являются клиентами компании;

— ПДн сотрудников Оператора.

В ИСПДн одновременно обрабатываются персональные данные менее чем 100000 субъектов персональных данных. Все информационные системы Оператора, кроме ИСПДн Сбис, являются локальными информационными системами, поскольку входящие в ее состав технические средства обработки информации размещены в пределах одного здания. В качестве среды передачи данных используется локальная сеть Оператора.

Информационная система персональных данных Оператора, функционирующая на базе АРМ специалистов кадровой службы, бухгалтерии обрабатывает следующую информацию о сотрудниках:

1) биографические сведения гражданина;

2) национальность;
3) религиозную принадлежность;
4) политические взгляды;
5) образование;
6) специальность;
7) занимаемую должность;
8) наличие судимостей;
9) адрес места жительства, домашний телефон;
10) состав семьи;
11) место работы;
12) размер заработной платы;
13) содержание трудового договора (контракта);
14) водительский стаж;
15) наличие автомобиля.

Концепция Политики защиты данных

1. Используемые технологии анализа
2. Объекты защиты

№ п/п	Название Объекта защиты	Состав объекта защиты

3. Списки отправителей/получателей

№ п/п	Название периметра	Список

4. Политики защиты данных

№ п/п	Название Политики	Тип политики (Политика защиты данных, Политика защиты данных на агентах)	Объекты защиты	Правила срабатывания

5. Правила агентского мониторинга

№ п/п	Правило	Описание правила

ПРОФЕССИОНАЛЬНОЕ КОНКУРСНОЕ ЗАДАНИЕ
ВАРИАТИВНАЯ ЧАСТЬ ЗАДАНИЙ

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины).

В ходе выполнения данного задания нужно установить и настроить ПО на рабочие станции будущей защищенной сети.

Настройки сетевого окружения

Для правильной работы сети надо создать или убедиться в наличии 4 сетей:

—Host only или внутренняя сеть адаптер для сети центрального офиса

—Host only или внутренняя сеть адаптер для сети филиала

—Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия

—Host only адаптер, NAT или Bridge для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)

IP адреса защищенных сетей

- Центральный офис «Сеть 1 ЦО»: 192.168.120.0/27
- Офис филиал «Сеть 1 Филиал»: 10.10.20.0/25
- Офис сеть 2 «Сеть 2 Офис»: 172.22.10.0/26
- «Интернет» для всех координаторов: 198.18.20.0/20

Адреса выбираются самостоятельно из указанного диапазона.

Необходимо записать все IP адреса, логины и пароли в этот файл.

На ВМ Net1-Admin установлена база данных с параметрами по умолчанию, Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ), Установлен клиент ЦУС. Необходимо восстановить структуру защищенной сети из файлов, подготовленных для миграции (расположены в папке Олимпиада на рабочем столе хостовой машины)

Установка ПО Coordinator и ПО Client для организации сети филиала уже произведена:

1. установлен ПО Coordinator HW-VA на Net1-Coord.

2. установлен ПО Client, ПО Publication Service, ПО Registration Point, ПО CA Informing рабочее место пользователя ВМ Net1-Oper.

Пароли для учетных записей ОС 111111.

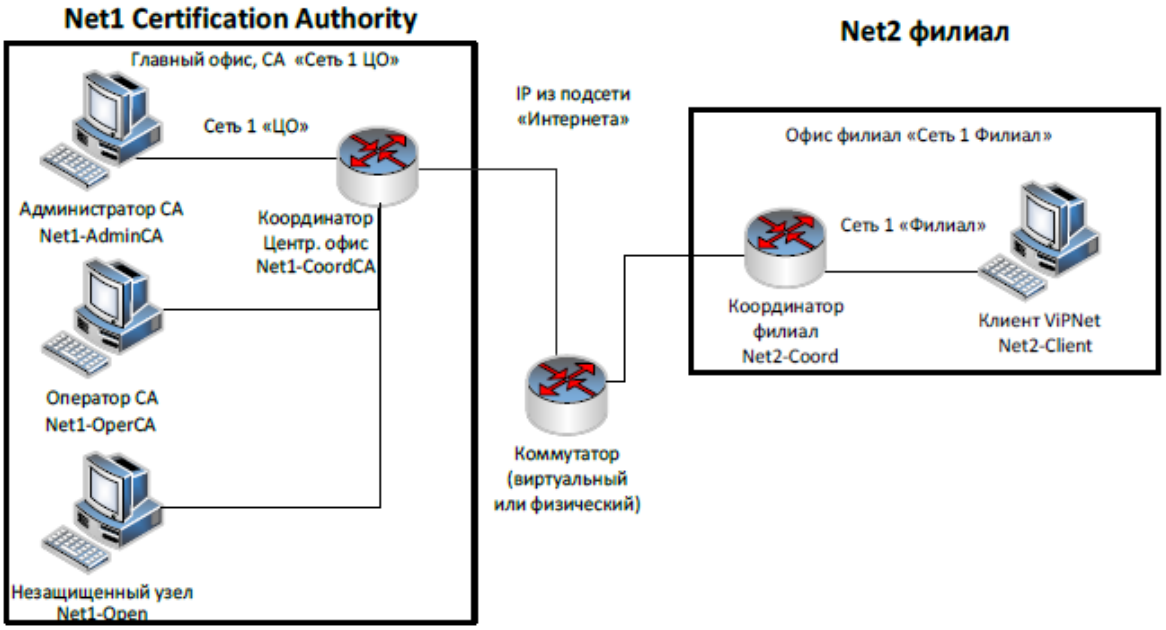
Восстановление структуры защищенной сети из файлов для миграции

Компоненты ViPNet Administrator были установлены на одном компьютере, их требуется перенести также на один компьютер. Необходимо использовать рабочее место администратора для восстановление структуры защищенной сети – все ПО установлено. Необходимо провести

инициализацию ПО, провести необходимые операции по восстановлению структуры сети из файлов для миграции.

В случае невозможности восстановления структуры сети, можно развернуть новую структуру сети с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями. Схема сети, которую можно создать, приведена далее.

При создании новой сети самостоятельно, баллы не назначаются.



В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing	ОС пользовательская или серверная	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	HW-VA	Coordinator C A
Net1-OperCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	ОС пользовательская или серверная	OperCA
Net2-CoordCA (Филиал)	Координатор Центр Офис (VM)	Coordinator	HW-VA	Coordinator C B
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	ОС пользовательска	UserCli

			я или серверная	

Связи между узлами необходимо настроить самостоятельно.

Схема связей пользователей	Coordinator CA	AdminCA	OperCA	Coordinator Subsidiary	UserCli
CoordinatorCA		+	+	+	
Admin CA	+		+		+
OperCA	+	+		+	
CoordinatorCB	+		+		+
UserCli		+		+	

Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

Рабочее место администратора (БД, ЦУС, УКЦ,Client)

- 1 координатор (Net3-Coord-HW-VA),
- 1 узел Admin (Net3-Admin) и пользователь Admin,
- Установите координатор.

Настройка политик безопасности в VipNet Policy Manager

Используя средство централизованного управления политиками безопасности, создать политику, которая разрешает узлу «UserCli» (Попов А.В.) трафик социальных сетей по будням: с часу до двух дня.

Создать шаблон политики безопасности для возможности подключения защищенных и незащищенных узлов своей сети по протоколу RDP к AdminCA (Валеев М.В.). Также необходимо включить RDP доступ на данном узле. Применить политику к устройствам.

Зафиксировать результат (скриншотами) настройки и проверки.

Настройка работы удостоверяющего центра в аккредитованном режиме. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации(Publication Service) и RegistrationPoint.

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

—сведения о средствах УЦ,

—средство электронной подписи издателя

—средства удостоверяющего центра

—сертификат на средство электронной подписи издателя Сертификат DemoVip.lab.crt

—сертификат на средство удостоверяющего центра Сертификат DemoVip.lab.p7b

—класс защищенности, которому соответствуют программные средства УЦ,

—место хранения контейнеров ключа ЭП и ключа защиты УКЦ

После перевода УКЦ в аккредитованный режим необходимо выпустить:

—Корневой квалифицированный сертификат. Назначить текущим.

—Квалифицированную электронную подпись для пользователя Admin. Выдать с новым дистрибутивом ключей.

—Квалифицированную электронную подпись для пользователя Client. Сохранить электронные ключи в файл.

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service). На машине Net1-OperCA уже развернут FTP-сервер (папка c:/Certs используется для FTP сервера). Для настройки обмена между УКЦ и Publication Service можно использовать преднастроенную общую папку c:/Published

Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL с периодичностью 1 день.

Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.

Посредством Центра Регистрации (Registration Point):

1. зарегистрировать пользователя UserCli;

2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;

3. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования (CA Informing):

4. настроить способ выдачи уведомлений;

5. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов

Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети

1. Добавить новый сетевой узел Ivanov и пользователя Ivanov за координатором ЦентрОфис. Добавить связь пользователя нового узла с пользователем UserCli (Попов А.В). На указанных узлах проверить появление нового узла. Установить ПО VipNet Client for Linux на ПК Astra и установить дистрибутивы ключей пользователя Ivanov. Отправить письмо деловой почты пользователю UserCli (Попов А.В.)

2. Добавить пользователя Petrov на узле UserCli (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи;

3. Отправить письмо по Деловой почте пользователю Petrov с узла Главный администратор.

4. Отправить текстовое сообщение пользователю Admin от пользователя Petrov

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

– скриншоты деловой почты на отправителе и получателе (при отправке письма);

– скриншоты текстового сообщения на отправителе и получателе;

– скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

1. Скомпрометировать ключи пользователя UserCli (Попов А.В.) на узле Пользователь_2 Филиал (Сотрудник Филиал),

2. Произвести смену ключей пользователя и сетевых узлов,

3. Отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (Сотрудник Филиал) (фиксировать все шаги),

4. Проверить работу защищенной сети после обновления отправив сообщение от пользователя UserCli (Попов А.В.) администратору (Валеев М.В).

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным

– указанным способом:

– компрометация пользователя.

– смена ключей пользователя и сетевых узлов.

– процедура смены ключа на клиенте с использованием резервного набора ключей.

скриншот экрана «защищенная сеть» в Monitor на узле Пользователь_2. Филиал (Попов А.В.) + результат проверки доступности узлов.

Кроме того, нужно сохранить архив директории, в которой расположен резервный набор ключей на рабочем столе компьютера (после смены ключей).

Настройте межсетевое взаимодействие с использованием индивидуального симметричного межсетевого мастер-ключа между сетью центрального офиса и филиала. Разрешите прохождение трафика в обоих направлениях локального незащищенного трафика между компьютерами.

Межсетевое взаимодействие защищённых сетей

Настроить межсетевое взаимодействие между двумя защищёнными сетями (N1 и N3), сделать скриншоты всех этапов установки межсетевого взаимодействия. Проверить взаимодействие узлов, отправив сообщение деловой почты в программе Client Monitor с узла.

Подключить незащищенную машину в сети N3 (Net3-Open). Для второй открытой машины использовать Net1-Open узел в сети 1. Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb (общая сетевая папка) или другим удобным (кроме ICMP); проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- Настройка максимального количества туннелей на координаторах
- Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
- Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования