МАКАРОВ П. А., БАЗАРОВА И. А. ПРИМЕНЕНИЕ ПРОДУКТОВ VIPNET PRIME ДЛЯ ФОРМИРОВАНИЯ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

УДК 004.056, ГРНТИ 81.93.29

Применение продуктов VipNet Prime для формирования защищенной информационной среды

П. А. Макаров[1], И. А. Базарова[2]

[1]ООО «Газинформсервис», г. Ухта;
[2]Ухтинский государственный технический университет, г. Ухта

Данная статья посвящена разработке макета защищенной сети. Развертывание макета осуществлялось с использованием продуктов ViPNet Prime, обеспечивающих безопасную передачу данных по интернет сети путем организации VPN соединения.

Ключевые слова: *ViPNet Prime, VPN, макет, xFfirewall, координатор, информационная безопасность*

Application of VipNet Prime products to create a secure information environment

P. A. Makarov[1], I. A. Bazarova[2]

[1]Gazinformservice LLC in Ukhta;
[2]Ukhta State Techincal University, Ukhta

This article is devoted to the development of a secure network layout. The layout was deployed using ViPNet Prime products, which ensure secure data transmission over the Internet by establishing a VPN connection

Keywords: *ViPNet Prime, VPN, layout, xFfirewall, coordinator, information security*

Введение

В данный момент защита сетей передачи данных является одним из важнейших компонентов информационной безопасности, так как существует риск перехвата или утечки информации. Угрозы кибербезопасности постоянно эволюционируют, представляя собой серьезную угрозу для конфиденциальности, целостности и передачи данных. Причины, почему защита информации имеет огромное значение: конфиденциальность, целостность, доступность, защита от киберугроз, соблюдение законодательства.

Обычно данные передаются через сеть Интернет. Публичные сети не гарантируют безопасность из-за различных угроз, которые могут возникнуть при передаче данных. В настоящее время существует множество методов для осуществления атак как на локальные сети, так и на передаваемую информацию.

Для безопасной передачи данных через интернет необходимо использовать технологию виртуальных частных сетей (VPN).

Цель исследования – описать реализацию защищённой информационной среды головного офиса и одного филиала кампании с использованием продуктов ViPNet Prime.

Предпроектное исследование

Сеть — это инфраструктура, в составе которой входят устройства и программное обеспечение. Сеть позволяет компьютерам и другим устройствам взаимодействовать друг с другом, передавать информацию и совместно использовать ресурсы, такие как файлы, Интернет-соединение, принтеры и прочее.

Так как информация будет передаваться не только в локальной, но и по общедоступной сети, то существует возможность для злоумышленников реализации различных атак, наиболее актуальными являются угрозы перехвата и анализа сетевого трафика.

Прослушивание трафика между сетями злоумышленниками, более известное как "sniffing", представляет собой вид кибератаки, при которой злоумышленник перехватывает и записывает данные, передаваемые между устройствами в сети. С помощью данного метода злоумышленник может получить конфиденциальную информацию, такую как пароли, данные банковских карт, личные сообщения и другие важные данные. В случае успешного прослушивания трафика злоумышленники могут использовать украденные данные для осуществления кибермошенничества, взлома аккаунтов или других противозаконных действий.

Так же должны применяться сертифицированные ФСБ и ФСТЭК, а также сертифицированных СКЗИ для обеспечения защиты информации.

СКЗИ (средства криптографической защиты информации) — это программы и устройства, которые шифруют и дешифруют информацию и проверяют, вносились ли в неё изменения. СКЗИ используют для безопасного хранения и передачи данных. С их помощью также создают электронные подписи.

Чтобы защитить информацию, её шифруют одним из криптографических алгоритмов.

Криптографический алгоритм - это метод или набор методов, используемых для шифрования и расшифровки информации. Этот метод позволяет защитить данные от несанкционированного доступа и предотвратить их передачу третьим лицам. При использовании криптографического алгоритма исходные данные преобразуются в зашифрованную форму, которую можно расшифровать только с помощью специального ключа. Существуют различные типы криптографических алгоритмов, каждый из которых имеет свои особенности и применяется в зависимости от конкретной ситуации.

Конфиденциальная информация — это сведения, доступ к которым ограничен законом РФ и которые не являются государственной тайной.

Конфиденциальными могут считаться персональные данные отдельного гражданина, служебные и коммерческие тайны предприятия, а также секретные сведения в правоохранительной сфере. Главные положения понятия конфиденциальности определяются законом № 149-ФЗ, который регламентирует соблюдение тайны, доступ к ней и ответственность за ее разглашение.

Все организации, от маленьких частных фирм до государственных корпораций, нуждаются в тщательной защите внутренней информации. Это обусловливается высоким уровнем недобросовестной конкуренции и промышленным шпионажем, когда похищенные сведения приводят к экономическому удару по компании.

Для защиты от несанкционированного доступа в локальные, а также для предотвращения возможных атак на внешние сети, необходимо будет установить на границы локальных сетей межсетевые экраны.

Межсетевой экран - это программно-аппаратное решение для защиты сетей или независимых устройств от различных кибератак и прочих угроз извне.

Основные функции межсетевого экрана:

– Предотвратить проникновение в сеть «поддельного» трафика. Межсетевой экран знает ip адреса локальной сети и если придёт трафик который замаскирован под данные внутренний сети, но отправлен с незнакомого IP. Межсетевой экран заметит это и не пропустит его внутрь локальной сети.

– Заблокировать передачу данных неизвестному источнику. Межсетевой экран не позволит отправить файл на не знакомый ip адрес во избежание утечки ценной информации.

Информация будет передаваться из между офисами по сети Интернет. Этот факт означает, что велик риск перехвата информации, вследствие чего может привести к анализу сетевого трафика злоумышленниками.

Для осуществления безопасной передачи данных необходимо будет построить туннели через общедоступную сеть (VPN), применить шифрование трафика, а также настроить сетевые фильтры на межсетевых экранах.

Туннелирование – технология, позволяющая защитить соединения между устройствами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих устройств не самими устройствами, а координаторами, которые установлены на границе их локальных сетей.

VPN – комплекс технологий, позволяющих создать логическую сеть поверх физической. Используется для обеспечения защиты трафика от перехвата злоумышленниками и безопасной деятельности в интернете.

Принцип работы VPN следующий:

– Аутентификация и установка соединения;

– Шифрование данных;

– Создание виртуального туннеля;

– Переадресация трафика.

Шифрование трафика – это механизм, обеспечивающий безопасную передачу трафика между устройствами CPE через туннели. Например, использование шифрование трафика при передаче данных между устройствами по туннелю, построенному поверх незащищенного Интернет-соединения.

Существует два основных типа шифрования:

– симметричное;

– асимметричное.

Основные продукты линейки, которые были использованы для развертывания защищенной сети [3]:

1. ViPNet Coordinator выполняет серверные функции, а также маршрутизацию трафика и служебной информации для обеспечения безопасной передачи данных между сегментами сети [8].

2. ViPNet xFirewall — шлюз безопасности, представляющий собой межсетевой экран класса NGFW (Next-Generation Firewall) с расширенными функциями анализа и фильтрации трафика. ViPNet xFirewall предназначен для комплексного решения задач информационной безопасности в корпоративных сетях за счет интеграции межсетевого экранирования, глубокой инспекции пакетов, системы предотвращения атак и контентной фильтрации [6].

3. ViPNet Client 4U for Linux предназначен для защиты каналов связи при подключении к защищенным с использованием технологии ViPNet ресурсам [7].

4. ViPNet Prime – единая система управления и эксплуатации продуктов Инфотекс. Технология ViPNet Prime, разработанная российской компанией «Инфотекс» [9].

Для реализации макета защищённой сети использовались виртуальные ViPNet xFirewall и ViPNet Coordinator.

Реализация макета защищенной сети

Так же была построена схема будущего макета защищённой сети (Рисунок 1).

MS Visio был выбран в качестве графического моделирования сети макета.

VMWare Workstation Pro была выбрана в качестве разработка макета с точки зрения программного обеспечения виртуализации.

Используемые операционные системы на виртуальных машинах:

– Astra Linux 1.7 (Смоленск) – для виртуальной машины администратора сети ViPNet Prime 1.7.2, ViPNet Client for Linux 4.14.0;

– ViPNet xFirewall 5.6.0 – для виртуальной машины межсетевой экран;

– ViPNet Coordinator VA 4.5.4 – для виртуальной машины координатора;

– Astra Linux 1.7 (Смоленск) – для виртуальной машины «Роутер» выполняющую маршрутизацию между офисами;

– Windows 10 – для пользовательских компьютеров, на которых не установлено программное обеспечение ViPNet Prime.

Развёртывание макета происходило в следующем порядке:

1) Установка ПО ViPNet Prime 1.7.2 с установкой следующих модулей: Universal Transport, Core, VPN, ViPNet Client for Linux, Dnsmasq (не входит в состав продуктов ViPNet Prime).

2) Создание структуры сети в модуле VPN и выдача дистрибутивов ключей.

3) Первичная инициализация ViPNet Client for Linux на ViPNet Prime;

4) Развёртывание 3 координаторов – ViPNet Coordinator VA 4.5.4;

5) Первичные настройки координаторов;

6) Развёртывание 2 межсетевых экранов – ViPNet xFirewall 5.6.0;

7) Первичные настройки межсетевых экранов;

8) Настройка маршрутизации трафика;
9) Развёртывание роутера в качестве маршрутизатора сетей;
10) Настройка сетевых параметров роутера;
11) Настройка туннелей между открытыми узлами;
12) Настройка фильтров на межсетевых экранах;
13) Настройка подключения координатора к внешней сети через межсетевой экран;
14) Настройка правил трансляции адресов;
15) Проверка работоспособности макета защищённой сети.

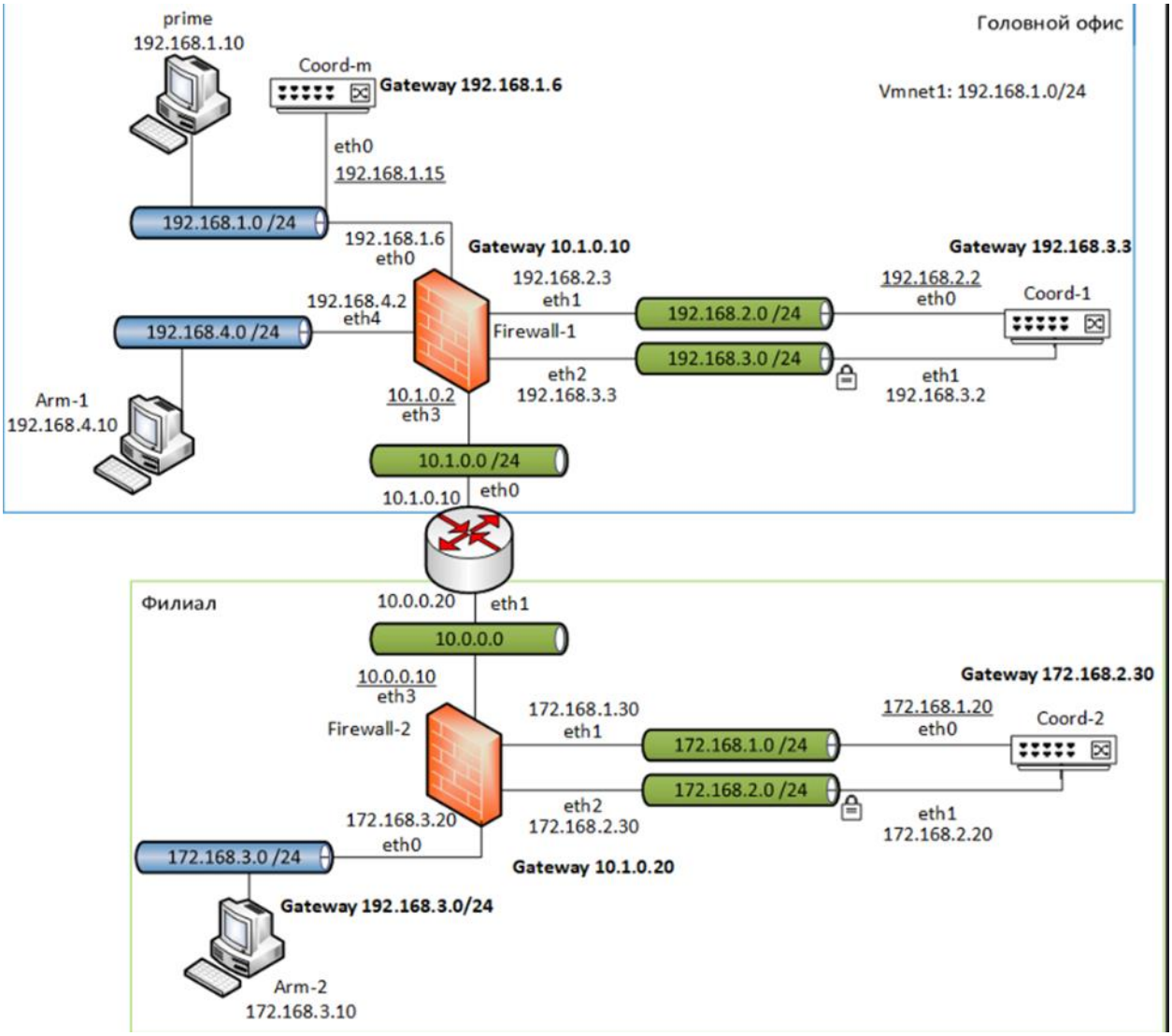

Рисунок 1. Макет сети

Результаты разработки

Результатом работы макета является сетевое взаимодействие между двумя локальными сетями с защищённой передачей данных между ними с использованием общедоступной сети Интернет.

Для проверки работоспособности макета был снят трафик с внутреннего и внешнего интерфейсов межсетевых экранов. Внешний интерфейс –сетевой

интерфейс eth3, направленный в сторону сети Интернет, внутренний – сетевой интерфейс eth0, направленный в сторону АРМа сотрудника локальной сети.

Для снятия трафика использовалась утилита tcpdump.

tcpdump – это штатная утилита UNIX, которая позволяет перехватывать и анализировать сетевой трафик, проходящий через устройство и вне устройства, на котором запущена данная утилита.

Для анализа сетевого трафика использовалась программа wireShark.

Для проверки защищённости трафика произведена передача файла с одного компьютера локальной сети в другую через Интернет. Файл «contract for services» был копирован в другую сеть с помощью сетевой папки.

После такого как файл был копирован, а трафик снят, данные файлы с трафиком откроем в программе wireShark. Сначала, открываем файл dump, где снят трафик с внешнего интерфейса. В качестве отправителя и получателя указаны белые адреса внешних интерфейсов файерволов, что скрывает реальную структуру внутренней сети. Кроме того, содержимое всех пакетов зашифровано, что исключает возможность хищения конфиденциальных сведений (Рисунок 2).

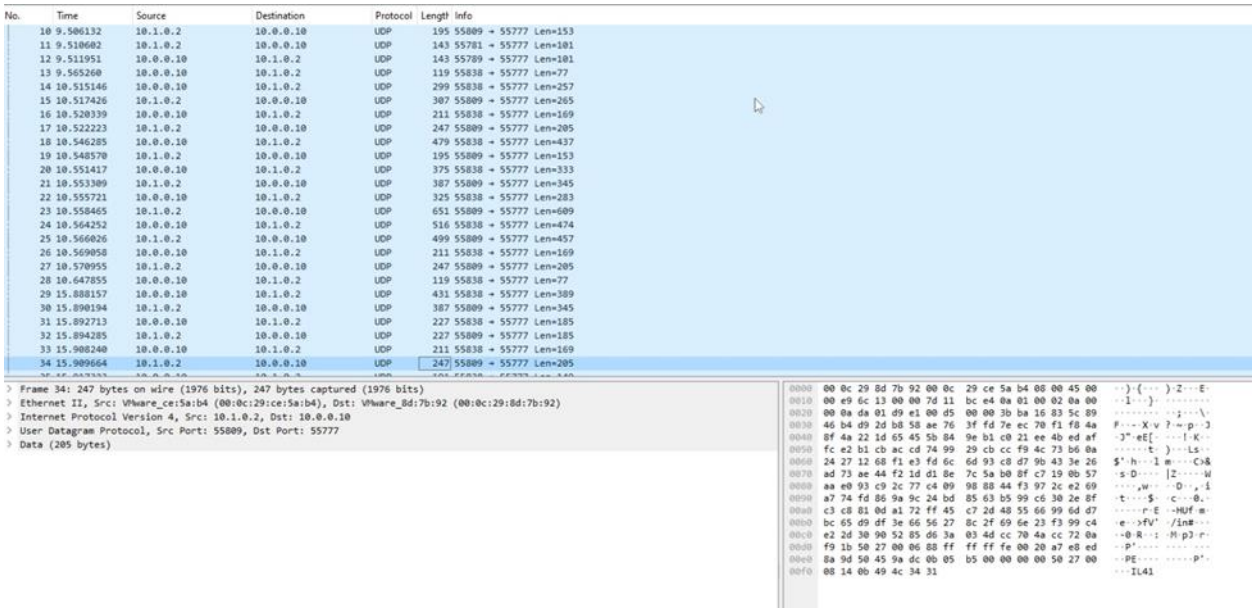

Рисунок 2. Зашифрованный трафик с внешнего интерфейса eth3

Трафик снятый с внутреннего интерфейса выглядит иначе: можем просмотреть адреса источников и получателей, типы отправляемых сообщений и используемые протоколы. В данном случае передача данных происходила по протоколу SMB2. Кроме того, было отображено имя передаваемого файла, также всё его содержимое, а именно наименование организации, номер договора, тип услуги и БИК (Рисунок 3).

Рисунок 3. Открытый трафик с внутреннего интерфейса eth0

Заключение

В данной статье было кратко описана разработка защищённой информационной среды с использованием продуктов ViPNet Prime.

Был проведён анализ предметной области, в ходе которого была выявлена необходимость в создании защищённой информационной среды.

В ходе работы произведена установка и настройка программного обеспечения ViPNet Prime, а также сопутствующих виртуальных машин.

Результатом является виртуальная сеть, с помощью которой можно безопасно передавать данные через общедоступную сеть Интернет. Чтобы убедиться в работоспособности данного макета была осуществлена проверка с помощью анализатора сетевого трафика Wireshark.

Список использованных источников и литературы

1. Аникин, Д. В. Защита информации в корпоративной сети с использованием технологии VPN / Д. В. Аникин. – Текст : электронный // Банковский бизнес и финансовая экономика: глобальные тренды и перспективы развития. – 2021. № 3. – С. 21-26.

2. Курсаков, О.В., Титов В.В., Емельянова М.М. Экспериментальное исследование эффективности защиты данных в беспроводной локальной сети Wi-Fi с помощью технологии ViPNet Prime / О.В. Курсаков, В.В. Титов, М.М.

Емельянова – Текст: электронный // Информационные технологии в науке, промышленности и образовании. Сборник трудов Всероссийской научнотехнической конференции. Ижевск, 2020. – С. 166–172.

3. Линейка продуктов VipNet Prime [Электронный ресурс]. – Режим доступа: https://infotecs.ru/product/ (дата обращения: 22.02.2024). 4 Чефранова А.О. Технология построения VPN VipNet: курс лекций: Учебное пособие. – Москва: Прометей, 2009. – 180 с.

4. Защита конфиденциальной информации: основные способы и мероприятия [Электронный ресурс]. – Режим доступа: https://gb.ru/blog/zaschita-konfidentsialnoj-informatsii/ (дата обращения: 04.04.2024).

5. Официальный сайт компании «ИнфоТеКС» | Безопасность информационных систем и защита данных, программное обеспечение [Электронный ресурс]. – Режим доступа: https://infotecs.ru/ (дата обращения: 01.02.2024).

6. Комплект документации ViPNet xFirewall 5.6.0 // Infotecs [Электронный ресурс]. – Режим доступа: https://infotecs.ru/downloads/documents/vipnet-xfirewall-5/. (дата обращения: 07.02.2024). – Текст: электронный

7. Комплект документации ViPNet Client for Linux 4.14.0 // Infotecs – [Электронный ресурс]. – Режим доступа: https://infotecs.ru/downloads/documents/vipnet-client-4u/ (дата обращения: 05.02.2024). – Текст: электронный

8. Комплект документации ViPNet Coordinator VA 4.5.4 // Infotecs [Электронный ресурс]. – Режим доступа: https://infotecs.ru/downloads/documents/vipnet-coordinator-va\. (дата обращения: 03.02.2024). – Текст: электронный

9. Комплект документации ViPNet Prime 1.7.2 // Infotecs Руководство по установке – Текст: электронный

List of references

1. Anikin, D. V. Information protection in a corporate network using VPN technology / D. V. Anikin. – Text : electronic // Banking business and financial economics: global trends and development prospects. 2021. No 3. PP. 21-26.

2. Kursakov, O.V., Titov V.V., Emelyanova M.M. Experimental study of the effectiveness of data protection in a wireless LAN Wi-Fi using ViPNet technology / O.V. Kursakov, V.V. Titov, M.M. Emelyanova Text: electronic // Information technologies in science, industry and education. 2020. PP. 166–172. URL: https://www.elibrary.ru/item.asp?id=43835845 (accessed: 05/15/2023).

3. ViPNet product line [Electronic resource]. Access mode: https://infotecs.ru/product / (accessed: 02/26/2023).

4. Chefranova A.O. Technology of building VPN ViPNet: a course of lectures: A textbook. Moscow: Prometheus, 2009. 180 p.

5. The official website of the Infotex company | Information systems security and data protection, software [Electronic resource]. – Access mode: https://infotecs.ru / (date of access: 02/01/2024).

6. ViPNet firewall 5.6.0 documentation set // Infotecs [Electronic resource]. – Access mode: https://infotecs.ru/downloads/documents/vipnet-xfirewall-5 /. (date of application: 02/07/2024). – Text: electronic

7. ViPNet Client for Linux 4.14.0 documentation kit // Infotecs – [Electronic resource]. – Access mode: https://infotecs.ru/downloads/documents/vipnet-client-4u / (date of access: 02/05/2024). – Text: electronic

8. ViPNet Coordinator VA 4.5.4 documentation set // Infotecs [Electronic resource]. – Access mode: https://infotecs.ru/downloads/documents/vipnet-coordinator-va \. (date of application: 02/03/2024). – Text: electronic

9. ViPNet Prime 1.7.2 Documentation Kit // Infotecs Installation Guide – Text: electronic