МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Информационных Технологий
Кафедра «Информационные системы и кибербезопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой, доктор PhD Мукашева А.К.

_____ «____» _____2021г.

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Построение защищенной корпоративной сети с применением технологий VPN

Специальность: Системы Информационной Безопасности

Выполнил: Швачунов Е.М. Группа: СИБдв-19-4

Научный руководитель: д.т.н., Ахметов Б. С.

Консультанты:
по экономической части:
к.э.н. д. Габелашвили К.Р_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
с.п. Абдрешов Ш. А._____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: с.п. Дмитриева М. В._____
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Алматы 2021

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Информационных Технологий

Кафедра «Информационные системы и кибербезопасности»

Специальность «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Швачунову Е.М.

Тема проекта «Построение защищенной корпоративной сети с применением технологий VPN»

Утверждена приказом по университету № 217 от «27» октября 2020 г.

Срок сдачи законченного проекта «1» июня 2021 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта):

1) Список оборудования существующей ИТ инфраструктуры;
2) Штатное расписание, регламенты компании.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:

1) Анализ предметной области;
2) Обзор кибер угроз;
3) Обзор технологий VPN;
4) Анализ решений на рынке.

Перечень графического материала (с точным указанием обязательных чертежей):

1) Скриншоты процесса установки и настройки оборудования;
2) Презентация (17 слайдов).

Основная рекомендуемая литература:

1) Ю. А. Родичев "Нормативная база и стандарты в области информационной безопасности" - Питер, 2017–256 с.
2) Е. К. Баранова, А. В. Бабаш Информационная безопасность и защита. Учебное пособие - РИОР, Инфра-М – 324 с

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Экономической части	Габелашвили К.Р.	01.03–03.05.21	
Безопасность жизнедеятельности	Абдрешов Ш. А.	14.03–03.05.21	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ угроз информационной безопасности	18.01.21	
Обзор VPN технологии	01.02.21	
Обзор методы построение VPN	15.02.21	
Анализ решений	26.02.21	
Установка и настройка оборудования	30.04.21	
Оформление отчета	07.05.21	
Создание презентации	10.05.21	

Дата выдачи задания «27» октября 2020г.

Заведующий кафедрой _____ Мукашева А. К.
(подпись)

Научный руководитель проекта _____ Ахметов Б. С.
(подпись)

Задание принял к исполнению студент _____ Швачунов Е.М.
(подпись)

АННОТАЦИЯ

Современная корпоративная сеть включает территориально распределенные узлы. Чтобы объединить их в единую сеть, нам нужны технологии, которые передают трафик в безопасном режиме. Концепция создания виртуальных частных сетей (VPN) активно развивается для обеспечения эффективного и безопасного использования сетевых атак в открытых сетях.

В дипломном проекте рассмотрены различные технологии, концепции построения и протоколы VPN. Показан пример построения корпоративной сети с помощью VPN, а также настройки оборудования.

Объект исследования – удаленный доступ к сети предприятия.

Цель работы – разработать инструмент удаленного доступа к корпоративной сети для увеличения защиты информации с помощью VPN технологий.

Методы исследования – теоретический анализ мер, предлагаемых всеми мировыми производителями ПО и оборудования по информационной безопасности, практическое моделирование в лабораторных условиях предложенного комплекса мер и имитация хакерских атак с целью проверки их работоспособности.

Результат – проанализированы технологии защиты корпоративных сетей, произведено проектирование, реализация, тестирование и обеспечение информационной безопасности сети предприятия.

АҢДАТПА

Қазіргі корпоративті желіге аумақтық бөлінген тораптар кіреді. Оларды бір желіге біріктіру үшін бізге трафикті қауіпсіз режимде өткізетін технологиялар қажет. Виртуалды жеке желілерді (VPN) құру тұжырымдамасы ашық желілердегі желілік шабуылдарды тиімді және қауіпсіз пайдалануды қамтамасыз ету үшін белсенді дамуда.

Дипломдық жобада әртүрлі VPN технологиялары, концепциялардың құрылымы және хаттамалары қарастырылған. VPN көмегімен корпоративтік желіні құру және жабдық параметрлері көрсетілген.

Зерттеу нысаны – кәсіпорын желісіне қашықтан қол жеткізу.

Жұмыстың мақсаты – VPN технологиялары көмегімен ақпаратты қорғауды арттыру үшін корпоративті желіге қашықтан қол жеткізу құралын жасау.

Зерттеу әдістері – бағдарламалық жасақтама мен ақпараттық қауіпсіздік жабдықтарының барлық әлемдік өндірушілері ұсынатын шараларды теориялық талдау, ұсынылған шаралар кешенін зертханалық жағдайда практикалық модельдеу және олардың жұмысын тексеру үшін хакерлік шабуылдарды модельдеу.

Нәтижесі – корпоративтік желілерді қорғау технологиялары талданып, кәсіпорын желісінің ақпараттық қауіпсіздігін жобалау, іске асыру, тестілеу және қамтамасыз ету жүргізілді.

ANNOTATION

The modern corporate network includes geographically distributed nodes. To combine them into a single network, we need technologies that transmit traffic in a secure mode. The concept of creating virtual private networks (VPNs) is being actively developed to ensure effective and secure use of network attacks in open networks.

The graduate project considers various technologies, construction concepts and protocols of VPN technologies. It contains an example of building a corporate network using the VPN, as well as configuring hardware.

The object of the study is remote access to the enterprise's network.

The goal is to develop a remote access tool to the corporate network to increase information protection through VPN technologies.

The research methods are theoretical analysis of the measures proposed by all global software and information security equipment manufacturers, practical modeling in the laboratory of the proposed set of measures and imitation of hacker attacks to verify their effectiveness.

The result is that corporate network protection technologies have been analyzed, the company's network has been designed, implemented, tested, and secured.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день, в период пандемии, COVID-19 угрожает не только здоровью людей, но и информационной безопасности компаний. Выполняемый в жатые сроки, массовый перевод сотрудников на удаленную работу, сопровождается значительными рисками. В момент изменения модели работы многие компании могут стать жертвами киберпреступников, которые используют ситуацию с коронавирусом в своих целях [1].

Актуальность проблематики информационной безопасности обусловлена синергетическим эффектом, главным образом определяемым двумя факторами (рисунок 1):

- всплеск невообразимого внимания к проблеме на уровне СМИ, что привело к резкому росту компьютерных вторжений, основанных на методах социальной инженерии;
- карантинные мероприятия, реализующие современные возможности удаленной работы, что изменило устоявшиеся режимы безопасного и устойчивого функционирования систем в Интернете [2].

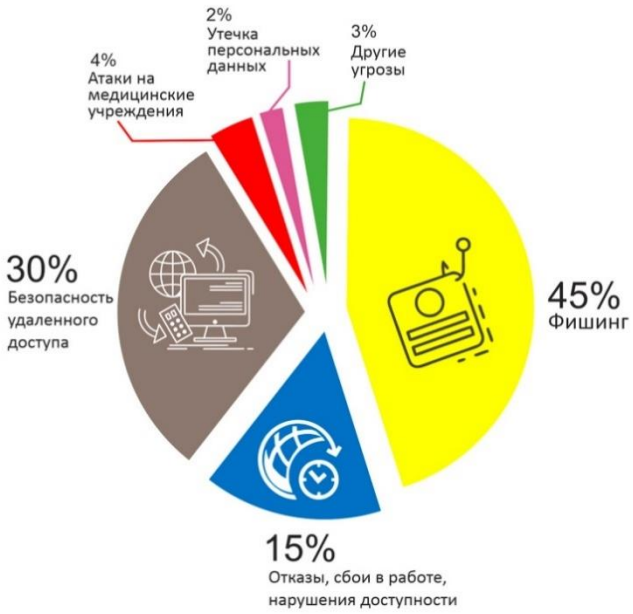


Рисунок 1 – Распределение угроз, релевантных коронавирусу, согласно упоминанию о них в Интернет

В таких ситуациях злоумышленники обычно пытаются найти уязвимости в первую очередь в решениях для удаленного доступа, подбирают пароли и ищут лазейки в веб-приложениях [3]. В результате увеличения спроса на облачные технологии, привело к увеличению DDoS-атак. Другой наиболее важной проблемой по мимо киберугроз при переходе на работу на дому, отсутствие возможности предоставления удаленного доступа к ресурсам компании. Что в свою очередь ведет к дополнительным расходам на закупку дорогостоящего оборудования и ПО, а также дополнительное время на

переконфигурирование сети предприятия и на обучение сотрудников грамотности по информационной безопасности при работе вне офиса.

Цель работы – разработать инструмент удаленного доступа к корпоративной сети для увеличения защиты информации с помощью VPN технологий.

1 Анализ угроз информационной безопасности

1.1 Постановка задачи

В соответствии с заданием на дипломное проектирование необходимо спроектировать корпоративную сеть основанную на VPN технологиях.

Корпоративная сеть (КС) — это сложная система, которая включает в себя множество компонентов.

КС могут иметь сложную топологию и могут располагаться в пределах города, региона, республики или даже континента. Количество пользователей, хостов и серверов также может измеряться сотнями или тысячами. Для подключения распределенных локальных сетей или отдельных компьютеров к единой корпоративной сети используются различные телекоммуникационные инструменты.

Основными задачами КС являются взаимодействие приложений, расположенных на разных хостах, а также доступ к этим приложениям удаленных пользователей. Развитая информационная система любого предприятия позволяет эффективно обрабатывать информационные потоки, циркулирующие между сотрудниками, и принимать своевременные и рациональные решения, обеспечивающие конкурентоспособность предприятия.

Основное отличие КС от локальной состоит в территориальном распределение сети. Если в пределах одного города можно рассчитывать на аренду выделенных линий, в том числе высокоскоростных, то при переходе на географически удаленные узлы стоимость аренды каналов становится баснословной, а их качество и надежность зачастую очень низки. Естественным решением этой проблемы является использование существующих глобальных сетей, таких как Интернет. В этом случае глобальная сеть возьмет на себя задачу доставки информации между узлами. Но, помимо низкой скорости и качества передачи, еще одной проблемой Интернета является его безопасность. Что является приводит к проблеме защиты корпоративной информации.

Цель работы – разработать инструмент удаленного доступа к корпоративной сети для увеличения защиты информации с помощью VPN технологий.

Как следует из цели работы, необходимо решить следующие задачи:

1) изучить существующую инфраструктуру и получить необработанные данные для проектирования сети с помощью VPN;
2) проанализировать риски;

3) на основе анализа рисков выбрать организационные и инженерные решения для повышения уровня информационной безопасности на предприятии;
4) описать процесс внедрения выбранных средств защиты информации с помощью VPN;
5) рассчитать экономическую эффективность внедряемых средств.

1.2 Социальная инженерия

Социальная инженерия — это психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. В целом, по словам эксперта Fortinet [4], атаки с использованием социальной инженерии – высокоэффективная и недорогая методика. Концептуально киберпреступники преследуют цели, аналогичные целям легального бизнеса – они стремятся получить максимальную прибыль при одновременном сокращении операционных расходов. А благодаря множеству вариантов вредоносного ПО, распространяемого как услуга, «as-a-Service» (программное обеспечение как услуга), доступного в Dark Web, атаки с использованием социальной инженерии идеально подходят для достижения этих целей.

Успешные атаки, в основе которых лежат методы социальной инженерии, направлены против базовых эмоциональных реакций людей, таких как «бей или беги». Когда человека переполняют такие чувства, как страх или сочувствие, он часто может принимать необдуманные решения. В начале пандемии киберпреступники использовали эти эмоции для проведения успешных фишинговых атак.

Атаки социальной инженерии бывают разных форм и могут выполняться везде, где задействовано человеческое взаимодействие. Рассмотрим наиболее распространенные формы атак цифровой социальной инженерии.

1.2.1 Приманка

Как следует из названия данный метод социальной инженерии использует ложные обещания, чтобы разжечь жадность или любопытство жертвы. Они заманивают пользователей в ловушку, которая крадет их личную информацию или заражает их системы вредоносным ПО [5, 6].

Мошенничество с приманкой чаще всего имеет материальную форму. Данная форма атаки использует физические носители для распространения вредоносных программ. Например, злоумышленники оставляют приманку – обычно зараженные вредоносным ПО флэш-накопители – в заметных местах, где потенциальные жертвы наверняка их увидят (например, ванные комнаты, лифты, парковка целевой компании). Приманка имеет аутентичный вид, например этикетку, на которой она изображена как ведомость заработной платы компании.

Жертвы из любопытства берут наживку и вставляют ее в рабочий или домашний компьютер, что приводит к автоматической установке вредоносного ПО в систему.

Мошенничество с приманкой не обязательно должно осуществляться в физическом мире. Онлайн-формы приманки включают в себя привлекательную рекламу, которая ведет на вредоносные сайты или побуждает пользователей загрузить приложение, зараженное вредоносным ПО.

1.2.2 Scareware (Лжеантивирус)

Пугающие программы (Scareware) включают в себя бомбардировку жертв ложными тревогами и вымышленными угрозами. Пользователи обманываются, думая, что их система заражена вредоносным ПО, предлагая им установить программное обеспечение, которое не имеет реальной пользы (кроме как для злоумышленника) или само является вредоносным ПО. Scareware также называют программным обеспечением для обмана, мошенническим программным обеспечением и программным обеспечением для сканирования.

Типичный пример пугающего ПО – это нормально выглядящие всплывающие баннеры, которые появляются в вашем браузере во время просмотра веб-страниц и содержат такой текст, как «Ваш компьютер может быть заражен вредоносными программами-шпионами». Он либо предлагает вам установить инструмент (часто зараженный вредоносным ПО), либо перенаправляет вас на вредоносный сайт, где заражается ваш компьютер.

Scareware также распространяется через спам-электронную почту, которая рассылает ложные предупреждения или предлагает пользователям купить бесполезные / вредные услуги.

1.2.3 Претекстинг

Здесь злоумышленник получает информацию с помощью серии искусно созданной лжи. Мошенничество часто инициируется злоумышленником, который притворяется, что ему нужна конфиденциальная информация от жертвы для выполнения важной задачи.

Злоумышленник обычно начинает с установления доверия со своей жертвой, выдавая себя за коллег, сотрудников полиции, банка, налоговых органов или других лиц, обладающих правом знать. Заявитель задает вопросы, которые якобы необходимы для подтверждения личности жертвы, с помощью которых они собирают важные личные данные.

С помощью этого мошенничества собирается всевозможная соответствующая информация и записи, такие как номера социального страхования, личные адреса и номера телефонов, записи телефонных разговоров, даты отпусков сотрудников, банковские записи и даже информация о безопасности, относящаяся к физическому объекту.

1.2.4 Фишинг

Как один из самых популярных типов атак социальной инженерии, фишинговые атаки представляют собой кампании по электронной почте и текстовым сообщениям, направленные на создание у жертв чувства срочности, любопытства или страха. Затем он побуждает их раскрыть конфиденциальную информацию, щелкнуть ссылки на вредоносные веб-сайты или открыть вложения, содержащие вредоносное ПО.

Примером может служить электронное письмо, отправленное пользователям онлайн-службы, которое предупреждает их о нарушении политики, требующем немедленных действий с их стороны, таких как обязательная смена пароля. Он включает ссылку на незаконный веб-сайт - почти идентичный по внешнему виду его законной версии - предлагая ничего не подозревающему пользователю ввести свои текущие учетные данные и новый пароль. После отправки формы информация отправляется злоумышленнику.

Учитывая, что идентичные или почти идентичные сообщения отправляются всем пользователям в фишинговых кампаниях, их обнаружение и блокировка намного проще для почтовых серверов, имеющих доступ к платформам обмена угрозами.

Целевой фишинг – это более адресная версия фишингового мошенничества, при котором злоумышленник выбирает конкретных лиц или предприятия. Затем они адаптируют свои сообщения на основе характеристик, должностей и контактов, принадлежащих их жертвам, чтобы сделать их атаку менее заметной. Целевой фишинг требует гораздо больших усилий со стороны злоумышленника и может занять недели и месяцы. Их гораздо труднее обнаружить, и они имеют больше шансов на успех, если делать это умело.

Сценарий целевого фишинга может включать злоумышленника, который, выдавая себя за ИТ-консультанта организации, отправляет электронное письмо одному или нескольким сотрудникам. Оно сформулировано и подписано точно так же, как обычно делает консультант, тем самым вводя получателей в заблуждение, заставляя думать, что это подлинное сообщение. В сообщении получателям предлагается сменить пароль и предоставляется ссылка, которая перенаправляет их на вредоносную страницу, где злоумышленник теперь перехватывает их учетные данные [7].

1.2.5 DDoS-атака

Распределенная атака типа «отказ в обслуживании» (DDoS) – это когда злоумышленник или злоумышленники пытаются сделать невозможным предоставление услуги. Этого можно добиться, заблокировав доступ практически ко всему: серверам, устройствам, службам, сетям, приложениям и даже конкретным транзакциям внутри приложений. При DoS-атаке вредоносные данные или запросы отправляет одна система; DDoS-атака исходит из нескольких систем.

Как правило, эти атаки работают, забивая систему запросами данных. Это может быть отправка веб-серверу такого количества запросов на обслуживание страницы, что он дает сбой по запросу, или это может быть база данных, пораженная большим объемом запросов. В результате доступная пропускная способность интернета, ресурсы ЦП и ОЗУ становятся перегруженными.

Существует три основных класса DDoS-атак:

1. Атаки на основе объемов используют огромные объемы фиктивного трафика для перегрузки такого ресурса, как веб-сайт или сервер. К ним относятся атаки ICMP, UDP и флуд-атаки с использованием поддельных пакетов. Размер атаки на основе объема измеряется в битах в секунду (бит / с).
2. DDoS-атаки на уровне протокола или сетевого уровня отправляют большое количество пакетов в целевые сетевые инфраструктуры и инструменты управления инфраструктурой. Эти атаки протокола включают, среди прочего, SYN-флуд и Smurf DDoS, и их размер измеряется в пакетах в секунду (PPS).
3. Атаки на уровне приложений проводятся путем переполнения приложений вредоносными запросами. Размер атак на уровне приложений измеряется запросами в секунду (RPS).

Хотя объем DDoS-атак со временем снизился, они по-прежнему представляют собой серьезную угрозу. Лаборатория Касперского сообщает, что количество DDoS-атак, обнаруженных Kaspersky DDoS Prevention в четвертом квартале 2020 года, несколько увеличилось по сравнению с аналогичным периодом 2019 года. Однако это на 31% меньше по сравнению с третьим кварталом 2020 года [8]. В 2020 году Cloudflare сообщает, что объем DDoS-атак увеличивался каждый квартал, кроме четвертого квартала [9].

По словам Касперского, недавно обнаруженные бот-сети, такие как Torii и DemonBot, способные запускать DDoS-атаки, вызывают беспокойство. Torii способен захватить ряд устройств IoT и считается более стойким и опасным, чем Mirai. DemonBot захватывает кластеры Hadoop, что дает ему доступ к большей вычислительной мощности.

Еще одна тревожная тенденция – появление новых платформ для запуска DDoS-атак, таких как 0x-booter. Этот DDos-as-a-service использует около 16 000 устройств Интернета вещей, зараженных вредоносным ПО Bushido, разновидностью Mirai.

Отчет о DDoS от Imperva показал, что большинство DDoS-атак в 2019 году были относительно небольшими. Например, атаки на сетевом уровне обычно не превышали 50 миллионов пакетов в секунду. Авторы отчета связывают это с услугами DDoS-наемника, которые предлагают неограниченные, но небольшие атаки. Imperva действительно наблюдала несколько очень крупных атак в 2019 году, включая атаку сетевого уровня, которая достигла 580 миллионов запросов в секунду, и атаку уровня приложений, которая достигла пика в 292000 запросов в секунду и длилась 13 дней [10].

Эта тенденция изменилась в четвертом квартале 2020 года, когда Cloudflare сообщила о «массовом росте» числа атак со скоростью более 500 Мбит / с и 50 000 пакетов в секунду. Эти атаки также стали более постоянными: в период с октября по декабрь наблюдалось почти 9% атак, которые длились более 24 часов.

Cloudflare также отметила то, что она назвала «деструктивной тенденцией» в увеличении количества атак RDDoS в 2020 году, когда организации получают угрозу DDoS-атаки, которая нарушит их работу, если не будет выплачен выкуп. Злоумышленники, как правило, нацелены на жертв, которые менее способны отреагировать и оправиться от такой атаки.

1.2.6 Атаки методом перебора. Метод грубой силы (brute force)

Атаки методом грубой силы часто выполняются скриптами или ботами, нацеленными на веб-сайт или страницу входа в приложение. Они циклически перебирают все возможные ключи или пароли. Общие приложения включают взлом паролей на веб-сайтах или в приложениях, шифрование или ключи API, а также вход по SSH [11].

Атака со взломом пароля – это только один шаг в цепочке уничтожения злоумышленника. Его можно использовать для получения доступа к учетным записям пользователей, электронной почты, банковских или SaaS-аккаунтов или для взлома API-интерфейсов или любой другой службы, требующей входа в систему и учетных данных.

Оттуда злоумышленник может выполнить намеченную цель. Успешная атака методом грубой силы дает злоумышленникам удаленный доступ к целевому компьютеру в сети. Основная цель этих злоумышленников – получить личную информацию, которая затем может быть использована для доступа к онлайн-учетным записям и сетевым ресурсам. Оттуда их можно использовать для отправки фишинговых ссылок, распространения поддельного контента или даже сбора учетных данных для продажи третьим лицам.

Процесс угадывания пароля для определенного сайта может быть трудоемкой и длительной задачей, поэтому хакеры разработали инструменты, которые помогут сделать эту работу быстрее. К ним относятся автоматизированные инструменты для помощи в атаках методом грубой силы, как Brutus, Medusa, THC Hydra, Ncrack, John the Ripper, Aircrack-ng и Rainbow.

Многие инструменты могут найти пароль из одного словарного слова за одну секунду. Подобные инструменты работают против многих компьютерных протоколов (таких как FTP, MySQL, SMPT и Telnet) и позволяют хакерам взламывать беспроводные модемы, определять слабые пароли, расшифровывать пароли в зашифрованном хранилище и переводить слова в лексикон; например, «don'thackme» превращается в «d0n7H4cKm3».

Успех атаки методом грубой силы измеряется временем, которое требуется для успешного взлома пароля. По мере увеличения длины пароля время, необходимое для его взлома, увеличивается в геометрической

прогрессии. Согласно Cloudflare, для взлома семизначного пароля при скорости 15 миллионов попыток ввода ключа в секунду потребуется 9 минут. На создание 13-значного пароля потребуется более 350 000 лет.

Аналогичным образом, чем длиннее ключ шифрования, тем больше времени и ресурсов требуется для его преодоления с помощью грубой силы. 128-битный ключ шифрования имеет 2128 возможных комбинаций, тогда как при 256-битном шифровании злоумышленник должен будет попробовать 2256 комбинаций. С современными технологиями, чтобы угадать их все, потребуются триллионы лет. Даже если злоумышленники используют графические процессоры, которые могут значительно увеличить количество попыток комбинаций в секунду, увеличение сложности паролей и использование надежного шифрования может увеличить время, необходимое для взлома пароля.

Типы атак методом перебора

- *Традиционные атаки методом грубой силы*: злоумышленник пробует все возможные комбинации.
- *Обратные атаки методом перебора*: небольшое количество общих паролей повторно проверяется на многих учетных записях.
- *Заполнение учетных данных*: атака пытается использовать украденные имена пользователей и пароли с сайтов или служб для взлома учетных записей в других службах и приложениях.
- *Атаки по словарю*: атака циклически перебирает слова из словаря или общие пароли от других утечек данных.
- *Атаки с использованием радужной таблицы*: используя предварительно вычисленный словарь паролей в виде открытого текста и соответствующих им хэш-значений, злоумышленники определяют пароли, обращая функцию хеширования.

Согласно отчету Verizon о расследованиях утечек данных за 2020 год, менее 20% взломов в рамках малых и средних предприятий связаны с применением грубой силы и менее 10% - для крупных организаций. Эта тенденция практически не изменилась по сравнению с итерациями отчета 2019 и 2018 годов, но пандемия коронавируса, возможно, изменила ситуацию.

В результате пандемии COVID-19 предприятия по всему миру приняли политику удаленной работы, которая оказала прямое влияние на пространство киберугроз. После массового перехода на удаленную работу киберпреступники пришли к логическому выводу, что количество плохо настроенных серверов RDP (протокол удаленного рабочего стола) возрастет, что приведет к увеличению числа атак.

С начала марта количество атак Bruteforce.Generic. RDP резко возросло по всему миру, и атаки на инфраструктуру удаленного доступа вряд ли прекратятся в ближайшее время - учитывая, сколько корпоративных ресурсов теперь доступно для удаленных сотрудников.

Хотя ни один метод не является надежным против атак методом грубой силы, организации могут принять множество мер, которые требуют больше времени и вычислительных ресурсов для атаки:

1. Использование длинных и сложных паролей, которые зашифрованы (в идеале с 256-битным шифрованием);
2. Используйте соль при хэширование паролей. Данный метод предназначен для хранения строк в отдельной базе данных и добавлении их к паролю перед его хешированием, чтобы у сотрудников с одним и тем же паролем были разные хэши;
3. Внедрите политику паролей, в которой будут учтены сложность паролей и повторное использование паролей в нескольких учетных записях;
4. Ограничьте попытки входа в систему в течение определенного периода времени или потребуйте сброса после определенного количества неправильных попыток;
5. Ограничьте время необходимое для аутентификации пароля;
6. Включите CAPTCHA;
7. По возможности включите многофакторную аутентификацию;
8. Рассмотрите возможность использования менеджера паролей.

2 VPN технологии

Доступ ко всем цифровым ресурсам, которые могут вам понадобиться, независимо от того, где вы находитесь и какое у вас подключение к сети, стало для большинства образом жизни. Независимо от того, являетесь ли вы компанией, которая делится данными с другими компаниями, или путешественником, которому необходимо постоянно оставаться на связи, доступ к ресурсам воспринимается как должное.

В то время как приложения, размещенные в общедоступном облаке, значительно упрощают определение местоположения, многие ресурсы размещаются в частном порядке по таким причинам, как безопасность и конфиденциальность. Доступ к этим частным ресурсам часто осуществляется через VPN (виртуальные частные сети).

Технология VPN – это простая идея: безопасно подключить человека, которому вы доверяете, к нужному ему ресурсу через сеть, которой вы не доверяете [12].

Задача заключается в том, чтобы знать, какой тип VPN и когда его использовать. Ниже рассмотрим два основных типа VPN: тип на основе клиента и тип на основе сети.

2.1 Типы клиентских VPN

VPN на основе клиента – это виртуальная частная сеть, созданная между отдельным пользователем и удаленной сетью. Для создания VPN-соединения

часто используется приложение. В большинстве сценариев пользователь вручную запускает VPN-клиент и аутентифицируется с помощью имени пользователя и пароля. Клиент создает зашифрованный туннель между компьютером пользователя и удаленной сетью. Затем пользователь получает доступ к удаленной сети через зашифрованный туннель. Примеры клиентских приложений VPN включают Cisco AnyConnect, Pulse (ранее Juniper) и GlobalProtect Palo Alto Networks.

Windows, Mac и мобильные операционные системы часто имеют встроенные стандартные опции клиента VPN. Например, Mac OS X 10.10 включает L2TP (протокол туннелирования уровня 2) поверх IPsec и PPTP (протокол туннелирования точка-точка). Даже Cisco IPsec, основанный на стандартах, плюс некоторые усовершенствования Cisco, является включенной опцией для пользователей Mac.

Обратите внимание, что хотя IPsec был предпочтительным клиентским протоколом VPN в течение многих лет, в наши дни чаще используется SSL. Например, Cisco больше не обновляет свой устаревший клиент IPsec. Вместо этого в главном клиентском решении Cisco для VPN, AnyConnect, используется протокол SSL.

Клиентские приложения VPN позволяют пользователям легко подключать свои ноутбуки или мобильные устройства к ресурсам компании из любого места. Это позволяет пользователю удаленно управлять своей сетью через защищенный VPN-туннель, проложенный между его устройством и брандмауэром компании.

Помимо базовых возможностей подключения, клиенты VPN часто предлагают расширенные функции безопасности. Один из них – это возможность тщательно проверить устройство пользователя, прежде чем подключать его к сети. Например, в процессе аутентификации клиент Cisco AnyConnect может проверить (помимо прочего), что на устройстве установлена определенная версия антивирусного программного обеспечения и что оно является частью определенного домена Windows. Это дает ИТ-отделам возможность отклонять клиентские VPN-устройства по причинам, отличным от простого сбоя аутентификации.

Премиум-клиенты VPN предоставляются за лицензионную плату. Хотя клиентское программное обеспечение может быть бесплатным, брандмауэр обычно лицензируется по количеству одновременных разрешенных подключений VPN. Например, у вас может быть 1000 VPN-клиентов, развернутых на устройствах ваших пользователей, но вам нужно только лицензировать брандмауэр для поддержки 500 из них в любой момент времени.

2.2 Типы сетевых VPN

Сетевые VPN – это виртуальные частные сети, которые безопасно соединяют две сети в ненадежной сети. Одним из распространенных примеров

является глобальная сеть на основе IPsec, где все офисы компании подключаются друг к другу через Интернет с помощью туннелей IPsec.

Есть несколько видов сетевых VPN. Мы рассмотрим три самых распространенных:

1. Туннели IPsec, как на основе маршрутов, так и на основе политик;
2. Динамические многоточечные VPN;
3. L3VPN на основе MPLS.

2.2.1 Туннели IPsec

Простейший вид сетевой VPN – это основанный на стандартах туннель IPsec, и большинство сетевых маршрутизаторов и брандмауэров могут его создать [13].

В принципе, туннель в сетевой VPN ничем не отличается от клиентского IPsec-туннеля. И сетевая, и клиентская реализации создают безопасный туннель, через который зашифрованный трафик проходит между сетями. В то время как туннель IPsec на основе клиента предназначен для инкапсуляции трафика для одного устройства, туннель IPsec на основе сети передает трафик для целых сетей устройств, позволяя им обмениваться данными.

Туннели IPsec, которые используют некоторые разновидности списков криптодоступа для определения трафика, который может проходить через них, обычно называются VPN на основе политик.

Задача VPN на основе политик заключается в том, чтобы списки криптодоступа обслуживались согласно требованиям бизнеса. Если новая IP-сеть подключается к сети, которой требуется доступ к сети на другой стороне туннеля, список криптодоступа должен быть обновлен на устройствах по обе стороны туннеля.

Используйте туннели IPsec на основе политик, когда вам нужно построить один туннель между двумя сайтами, чтобы обеспечить тщательно контролируемый доступ к ресурсам. Туннели IPsec используются на основе политик в следующих ситуациях:

- чтобы подключиться к другой компании, выполняющей работу для вашей компании;
- в качестве резервной копии частного канала между удаленными офисами;
- в качестве временного подключения к новому объекту, введенному в эксплуатацию во время корпоративного слияния;
- в качестве связи для сотрудников на удаленной работе.

В отличие от туннелей IPsec на основе политик, туннели IPsec на основе маршрутов больше похожи на виртуальный канал, позволяющий любому трафику проходить через них. VPN на основе маршрутов доступны от многих поставщиков сетевых услуг, включая Cisco и Juniper. Однако доступность зависит от платформы. Например, Cisco ASA не поддерживает VPN на основе маршрутов.

Хотя IPsec VPN основаны на стандартах, производители, к сожалению, часто применяют стандарты по-разному. Поэтому создание туннеля IPsec VPN между устройствами от двух разных поставщиков – это своего рода обряд для сетевых инженеров.

Можно потратить много часов, пытаясь установить туннели IPsec между оборудованием Cisco и Checkpoint или Juniper. Это можно сделать, но часто бывает сложно прочесать детали конфигурации и сообщения журнала, чтобы найти проблему, которая мешает формированию туннеля.

2.2.2 L3VPN на основе MPLS

L3VPN наиболее часто развертываемое приложение в многопротокольных сетях с коммутацией меток (MPLS) [14].

MPLS чаще всего встречается в сетях поставщиков услуг, таких как AT&T, Verizon Business, Level 3 и CenturyLink. MPLS позволяет поставщикам услуг виртуализировать свои сети, чтобы клиенты могли совместно использовать физическую сеть, но при этом оставаться логически разделенными. MPLS не ограничивается поставщиками услуг; некоторые крупные предприятия используют MPLS внутри своих собственных глобальных инфраструктур [15].

Если ваша компания получает услугу WAN от поставщика услуг, он, скорее всего, предлагает вашей компании услуги L3VPN через свою сеть MPLS. В этом сценарии каждый офис в вашей компании подключается к поставщику услуг через то, что поставщик услуг видит, как клиентский маршрутизатор – тот, который соединяет канал WAN от поставщика услуг с остальной частью вашей сети.

На другом конце канала WAN находится граничный маршрутизатор провайдера (PE). Маршрутизатор PE отбрасывает трафик из канала вашей компании в экземпляр виртуальной переадресации маршрута (VRF), который является уникальным для вашей компании, а затем перенаправляет его в основной маршрутизатор провайдера, используя MPLS для маркировки трафика и определения VRF, которому принадлежит трафик.

Ядро провайдера доставляет трафик через свое ядро на другой маршрутизатор PE, затем на другой из ваших маршрутизаторов WAN, где ваш маршрутизатор затем доставляет трафик в сеть удаленного офиса.

Для вашей компании этот L3VPN невидим. Вам не нужно запускать MPLS. Вы не видите, как трафик безопасно перенаправляется через магистраль провайдера. Вы можете взаимодействовать с провайдером, используя маршрутизацию OSPF или BGP, чтобы объявить им свои маршруты, которые они будут переносить в уникально назначенном вам VRF. Но, кроме этого, вы знаете только, что ваш трафик идет в один маршрутизатор и выходит через другой.

Хотя создание DMVPN через Интернет является жизнеспособным решением для подключения, интернет-сервис может быть не таким надежным,

как требуется вашей компании, в зависимости от ваших требований. Провайдер услуг может определять приоритеты голосового и видеотрафика (при условии, что он отмечен соответствующим образом), в то время как Интернет не может сделать такой дифференциации.

С другой стороны, полоса пропускания интернета значительно дешевле по сравнению с пропускной способностью частной глобальной сети, работающей через службу L3VPN оператора. По этой причине многие предприятия время от времени соглашаются с риском плохого качества сети и отказываются от своих частных глобальных сетей в пользу некоторой разновидности VPN через Интернет.

2.3 Методы создания VPN

Поскольку VPN создает безопасный «туннель» через общедоступную сеть, протоколы, используемые для установления этого туннелированного соединения, называются протоколами туннелирования. Пять наиболее распространенных методов создания виртуальной частной сети включают в себя [16]:

1. PPTP;
2. L2TP;
3. IPSec;
4. SSL.

К сожалению, не существует однозначного универсального решения. Наилучший выбор для вашей организации зависит от ряда факторов: развернутых серверных и клиентских операционных систем, сетевых ресурсов, к которым необходим доступ, требуемого уровня безопасности, проблем с производительностью, административных накладных расходов и т. д.

2.3.1 PPTP

Протокол туннелирования точка-точка (PPTP), разработанный Microsoft совместно с другими технологическими компаниями, является наиболее широко поддерживаемым методом VPN среди клиентов Windows и единственным протоколом VPN, встроенным в операционные системы Windows 9x и NT. PPTP – это расширение стандартного Интернет-протокола Point-to-Point (PPP), протокола канального уровня, используемого для передачи IP-пакетов по последовательным каналам. PPTP использует те же типы аутентификации, что и PPP (PAP, SPAP, CHAP, MS-CHAP, EAP).

PPTP устанавливает туннель, но не обеспечивает шифрование. Он используется вместе с протоколом Microsoft Point-to-Point Encryption (MPPE) для создания безопасной VPN. PPTP имеет относительно низкие накладные расходы, что делает его быстрее, чем некоторые другие методы VPN.

Поскольку клиентское программное обеспечение встроено в большинство операционных систем Microsoft, серверы PPTP можно развернуть, не беспокоясь об установке клиентского программного

обеспечения в этих системах. Клиенты PPTP также доступны для Linux [17] и Macintosh OS 9.x. Mac OS X 10.2 поставляется со встроенной поддержкой PPTP, а также доступны сторонние клиенты для OS X. PPTP VPN поддерживаются многими основными устройствами межсетевого экрана и программными межсетевыми экранами корпоративного уровня, включая ISA Server, Cisco PIX, SonicWall и некоторые модели WatchGuard.

PPTP в прошлом подвергался критике за различные недостатки безопасности; многие из этих проблем решены в текущих версиях протокола. Использование аутентификации EAP значительно повышает безопасность PPTP VPN. Одним из преимуществ использования PPTP является отсутствие необходимости в инфраструктуре открытых ключей; однако EAP действительно использует цифровые сертификаты для взаимной аутентификации (как клиентской, так и серверной) и максимальной безопасности.

2.3.2 L2TP

Протокол туннелирования уровня 2 (L2TP) был разработан в сотрудничестве между Cisco и Microsoft и сочетает в себе функции PPTP с функциями проприетарного протокола Cisco Layer 2 Forwarding (L2F). Одним из преимуществ L2TP над PPTP является то, что его можно использовать в сетях без IP, таких как ATM, Frame Relay и X.25. Как и PPTP (и как следует из его названия), L2TP работает на канальном уровне сетевой модели OSI. L2TP VPN поддерживаются многими основными продуктами межсетевого экрана, включая ISA Server, CheckPoint, Cisco PIX и WatchGuard.

Клиент L2TP встроен в Windows 2000, XP и 2003, но вы можете загрузить клиентское программное обеспечение для большинства операционных систем, предшествующих Windows 2000 (Windows 98, ME и NT 4.0).

IP Security (IPSec), а точнее его протокол Encapsulating Security Payload (ESP), обеспечивает шифрование для туннелей L2TP.

L2TP требует использования цифровых сертификатов. Аутентификация пользователя может выполняться с помощью тех же механизмов аутентификации PPP, что и PPTP, но L2TP также обеспечивает аутентификацию компьютера. Это добавляет дополнительный уровень безопасности.

L2TP имеет несколько преимуществ перед PPTP. PPTP обеспечивает конфиденциальность данных, но L2TP идет дальше и также обеспечивает целостность данных (защита от изменения данных между моментом, когда они покинули отправитель, и моментом, когда они достигли получателя), аутентификация происхождения (подтверждение того, что пользователь, который утверждает, что имеет отправил данные, действительно сделал), и защиту от воспроизведения (которая не позволяет хакеру перехватить отправленные данные, такие как отправка учетных данных, а затем «воспроизвести» их, чтобы «обмануть» сервер). С другой стороны, накладные

расходы, связанные с обеспечением этой дополнительной безопасности, могут привести к несколько более низкой производительности, чем PPTP.

2.3.3 IPSec

Администраторы Windows знают IPSec как протокол, используемый для шифрования в сочетании с протоколом туннелирования L2TP. Однако IPSec сам по себе может использоваться в качестве протокола туннелирования, и на самом деле многие считают его «стандартным» решением VPN, особенно для виртуальных частных сетей типа «шлюз-шлюз» (site-to-site), которые соединяют две локальные сети. IPSec работает на более высоком уровне модели OSI, сетевом уровне (уровень 3) [18].

Многие аппаратные устройства VPN используют реализацию IPSec. Например, концентраторы Cisco VPN и межсетевые экраны PIX поддерживают IPSec, как и устройства NetScreen, SonicWall и WatchGuard. Программные брандмауэры корпоративного уровня, такие как ISA Server, CheckPoint и Symantec Enterprise Firewall, также поддерживают IPSec VPN.

IPSec в туннельном режиме защищает пакеты, которые передаются между двумя шлюзами или между клиентским компьютером и шлюзом. Как следует из названия, IPSec VPN работает только с IP-сетями и приложениями. Подобно PPTP и L2TP, IPSec требует, чтобы на клиентских компьютерах VPN было установлено клиентское программное обеспечение.

Аутентификация выполняется через протокол обмена ключами в Интернете (IKE) либо с цифровыми сертификатами (что является более безопасным методом), либо с предварительным ключом. IPSec VPN может защитить от многих наиболее распространенных методов атак, включая отказ в обслуживании (DoS), повторное воспроизведение и атаки типа «человек посередине» [19].

Многие поставщики включают в свое программное обеспечение VPN-клиента функции «управляемого клиента», которые позволяют вам устанавливать политики в отношении таких вещей, как требование, чтобы на клиентском компьютере было установлено антивирусное программное обеспечение или персональный брандмауэр, чтобы иметь возможность подключаться к шлюзу VPN.

Поддержка IPSec включена в Windows 2000 / XP / 2003, но не в более старые операционные системы Windows. Поставщики шлюзов VPN, такие как Cisco и CheckPoint, предоставляют клиентское программное обеспечение для своих виртуальных частных сетей на основе IPSec. Обратите внимание, что вам может потребоваться приобрести лицензии на клиентское программное обеспечение.

2.3.4 SSL

Популярность технологии VPN становится все более популярной – это Secure Sockets Layer (SSL) VPN. Большим преимуществом SSL VPN является

то, что вам не нужно специальное клиентское программное обеспечение VPN на клиентах VPN. Это потому, что SSL VPN использует веб-браузер в качестве клиентского приложения. Таким образом, SSL VPN известны как «бесклиентские» решения. Это также означает, что протоколы, которые может обрабатывать SSL VPN, более ограничены. Однако это также может быть преимуществом с точки зрения безопасности. С помощью SSL VPN вместо того, чтобы предоставлять VPN-клиентам доступ ко всей сети или подсети, как в случае с IPSec, вы можете ограничить их доступ к определенным приложениям. Однако если приложения, к которым вы хотите предоставить им доступ, не основаны на браузере, может потребоваться специальное программирование для создания подключаемых модулей Java или Active-X, чтобы сделать приложение доступным через браузер. Недостатком этого является то, что для использования таких подключаемых модулей настройки браузера клиента должны быть открыты, чтобы разрешить активный контент, что подвергает браузер воздействию вредоносных апплетов, если вы не настроите его на блокировку неподписанного активного содержимого и убедитесь, что плагины имеют цифровую подпись.

SSL VPN работают на еще более высоком уровне модели OSI, чем IPSec VPN на уровне сеанса. Это дает им возможность более детально контролировать доступ. SSL VPN используют цифровые сертификаты для аутентификации сервера. Для аутентификации клиента могут использоваться и другие методы, но сертификаты предпочтительнее как наиболее безопасные.

Несмотря на то, что не установлено клиентское программное обеспечение (кроме веб-браузера), шлюзы SSL VPN по-прежнему могут обеспечивать преимущества «управляемых клиентов», заставляя браузер запускать апплеты, например, для проверки наличия антивирусного программного обеспечения. прежде, чем можно будет установить VPN-соединение.

3 Виды аутентификаций и безопасность сети

Некоторые из крупнейших утечек данных за последние два года, в том числе затрагивающие Target, Home Depot и почтовую службу США, были результатом того, что хакеры получили доступ через виртуальные частные сети (VPN).

Между поставщиками, подрядчиками, сотрудниками, работающими удаленно, и сотрудниками, пользующимися преимуществами политик «принеси свое собственное устройство», средняя компания имеет множество пользователей и устройств, получающих доступ к VPN. Это делает их основной мишенью для похитителей данных и серьезной уязвимостью для вашей организации.

Для большинства фирм разрешение доступа с использованием только имени пользователя и пароля больше не является адекватным методом аутентификации пользователей, поскольку эта информация может быть легко

получена и использована хакерами. С годами появились более надежные методы аутентификации, в том числе:

1. *Двухфакторная аутентификация*. Этот метод обеспечивает дополнительный уровень безопасности, при этом обеспечивая удобный доступ для авторизованных пользователей. Наиболее распространенной формой двухфакторной аутентификации является получение пользователем текстового сообщения или SMS на свой телефон с кодовым номером. Этот код автоматически отправляется пользователю после того, как он или она введет свое стандартное имя пользователя и пароль. Стандарт безопасности данных индустрии платежных карт (PCI DSS) требует двухфакторной аутентификации для удаленного доступа к сети сотрудников, администраторов и третьих лиц;
2. *Риск-ориентированная аутентификация (RBA)*. Этот метод применяет различные уровни аутентификации в зависимости от риска взлома системы. Чем выше риск для системы, тем выше требуется уровень аутентификации. Например, людям, которые пытаются получить доступ к банковским счетам из другой страны, могут быть заданы дополнительные вопросы безопасности для подтверждения их личности. Дополнительные протоколы аутентификации также могут применяться на основе IP-адреса пользователя или из-за отсутствия антивирусного программного обеспечения;
3. *Протокол аутентификации с вызовом рукопожатия (CHAP)*. CHAP использует схему хеширования MD5 для шифрования аутентификации. При использовании протокола CHAP фактический пароль не пересылается по сети. Вместо этого он использует механизм запрос-ответ с односторонним хешированием MD5. CHAP защищает от атак повторного воспроизведения за счет использования постепенно изменяющегося идентификатора и переменного значения запроса. У Microsoft есть проприетарная версия CHAP под названием MS-CHAP;
4. *Служба удаленной аутентификации пользователей с телефонным подключением (RADIUS)*. Этот метод позволяет серверам удаленного доступа взаимодействовать с центральным сервером для аутентификации пользователей. В центральной базе данных хранятся профили пользователей, которые могут совместно использоваться всеми удаленными серверами. RADIUS позволяет компании настроить политику, которая может применяться в одной администрируемой точке сети;
5. *Смарт-карты*. Смарт-карты – это физические ключи с чипами, которые могут хранить информацию для входа в систему. Пользователи вставляют смарт-карты в считывающее устройство, подключенное к сети, а затем используют личный идентификационный номер (PIN) для получения доступа, подобно

тому, как работает карта банкомата. Смарт-карты можно комбинировать с удостоверением личности сотрудника, чтобы у них была одна карта для доступа в здание и сеть;

6. *Kerberos*. Этот процесс аутентификации на основе билетов, разработанный в Массачусетском технологическом институте (MIT), хранит пароли на централизованном сервере и предоставляет билеты для доступа. Это делается с помощью различных уровней шифрования. И пользователь, и сервер проверяют авторизованные личности друг друга, что может происходить в незащищенной сети. После идентификации связь между пользователем и сервером может быть зашифрована для обеспечения конфиденциальности и целостности данных [20];
7. *Биометрия*. Один из наиболее надежных методов аутентификации с использованием личных физических атрибутов пользователя, таких как отпечаток пальца, сканирование сетчатки глаза или распознавание голоса;
8. *Аутентификация на основе токенов*. Технологии аутентификации на основе токенов позволяют пользователям один раз ввести свои учетные данные и получить взамен уникальную зашифрованную строку случайных символов. Затем вы можете использовать токен для доступа к защищенным системам вместо того, чтобы заново вводить свои учетные данные. Цифровой токен доказывает, что у вас уже есть разрешение на доступ. Сценарии использования аутентификации на основе токенов включают RESTful API, которые используются несколькими платформами и клиентами.

3.1 Kerberos

Kerberos – это протокол аутентификации для клиент-серверных приложений. Этот протокол основан на комбинации шифрования закрытого ключа и билетов доступа для безопасной проверки личности пользователя [21].

Основными причинами использовать Kerberos являются [22]:

1. Простые текстовые пароли никогда не передаются по небезопасной сети;
2. Каждый логин имеет три этапа аутентификации;
3. Шифрование защищает все ключи доступа и билеты;
4. Аутентификация является взаимной, поэтому и пользователи, и поставщики защищены от мошенничества.

MIT разработал первые экземпляры Kerberos в конце 80-х. Протокол был назван в честь Цербера, существа из греческой мифологии. Цербер был свирепым трехголовым псом, охранявшим Аида.

Усовершенствованная версия Kerberos вошла в Microsoft как часть Windows 2000. С тех пор Kerberos стал протоколом авторизации Windows по умолчанию. Реализации Kerberos также существуют для Apple OS, FreeBSD,

UNIX и Linux. Консорциум Kerberos рассматривает протокол как проект с открытым исходным кодом.

Каждая проверка Kerberos включает в себя Центр распределения ключей (KDC). KDC действует как доверенная сторонняя служба аутентификации и работает с сервера Kerberos. KDC состоит из трех основных компонентов:

1. Сервер аутентификации (AS): AS выполняет начальную аутентификацию, когда пользователь хочет получить доступ к службе;
2. Сервер предоставления билетов (TGS): Этот сервер соединяет пользователя с сервером обслуживания (SS);
3. База данных Kerberos: Эта база данных хранит идентификаторы и пароли проверенных пользователей.

Описание потока (рисунок 2) [23]:

1. Клиент Kerberos отправляет свой идентификатор пользователя в виде открытого текстового сообщения в AS. Сообщение не содержит ни пароля клиента, ни его секретного ключа, основанного на этом пароле;
2. AS проверяет, находится ли клиент в базе данных пользователей, и если он найден, генерирует секретный ключ для клиента, хэшируя пароль клиента. Затем AS отправляет ключ сеанса client/TGS и TGT клиенту Kerberos. Сеансовый ключ шифруется секретным ключом клиента;
3. Клиент Kerberos расшифровывает ключ сеанса клиента/TGS и отправляет сообщение запроса, содержащее TGT и идентификатор службы Kerberos, к которой необходимо получить доступ, а также сообщение аутентификатора, содержащее идентификатор клиента и метку времени и зашифрованное с помощью ключа сеанса клиента/TGS в TGS;
4. TGS расшифровывает TGT в сообщении запроса для получения ключа сеанса клиента/TGS и расшифровывает сообщение аутентификатора. TGS проверяет, что клиент Kerberos авторизован для доступа к запрошенной службе Kerberos, и отправляет клиенту Kerberos билет службы и ключ сеанса клиент/сервер, зашифрованный с помощью ключа сеанса клиент/TGS;
5. Клиент Kerberos отправляет билет службы и новое сообщение аутентификатора, зашифрованное с помощью ключа сеанса клиент/сервер, в службу Kerberos для доступа;
6. Служба Kerberos расшифровывает билет службы, чтобы получить ключ сеанса клиент/сервер, а затем расшифровывает сообщение аутентификатора, чтобы получить временную метку клиента. Служба Kerberos отправляет клиенту Kerberos сообщение подтверждения службы, включающее метку времени и зашифрованное с помощью ключа сеанса клиент/сервер;
7. Клиент Kerberos расшифровывает сообщение подтверждения службы и проверяет правильность временной метки. Взаимная аутентификация теперь завершена. Теперь клиент Kerberos может

начать выдавать запросы на обслуживание, а служба Kerberos может предоставлять клиенту запрошенные услуги.

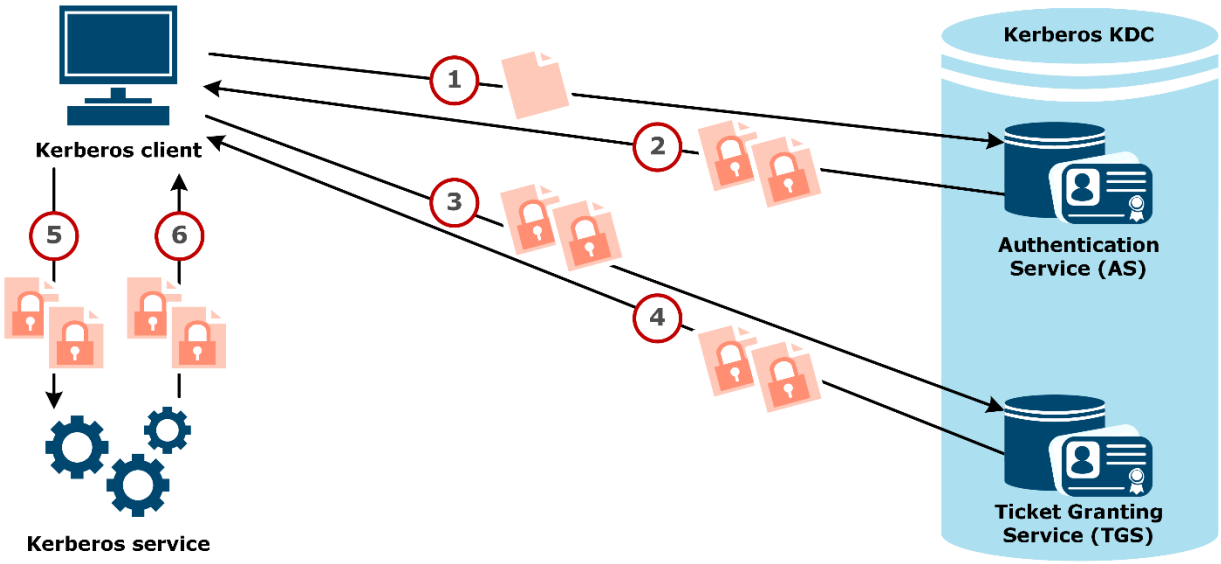


Рисунок 2 - Описание потока Kerberos

Все проверки подлинности Kerberos происходят в областях Kerberos. Область – это группа систем, над которыми KDC имеет полномочия проверять пользователей и службы (рисунок 3).

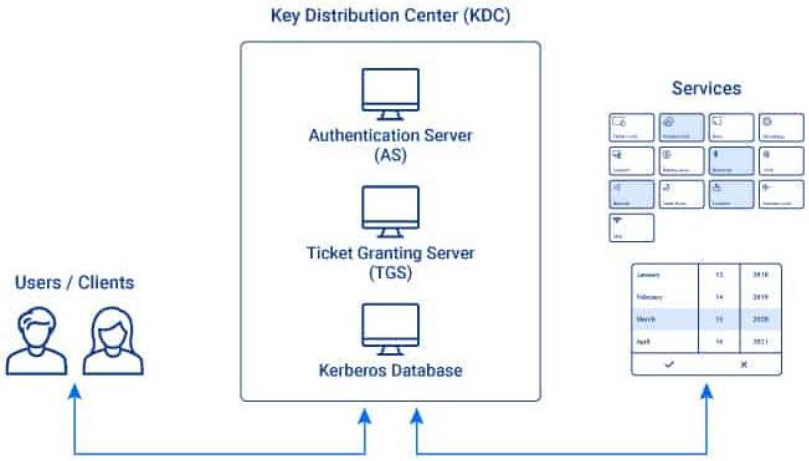


Рисунок 3 – Область Kerberos

Kerberos работает как с симметричной, так и с асимметричной криптографией (с открытым ключом). Протокол также может обрабатывать многофакторную аутентификацию (MFA).

Аутентификация Kerberos – это многоступенчатый процесс (рисунок 4).

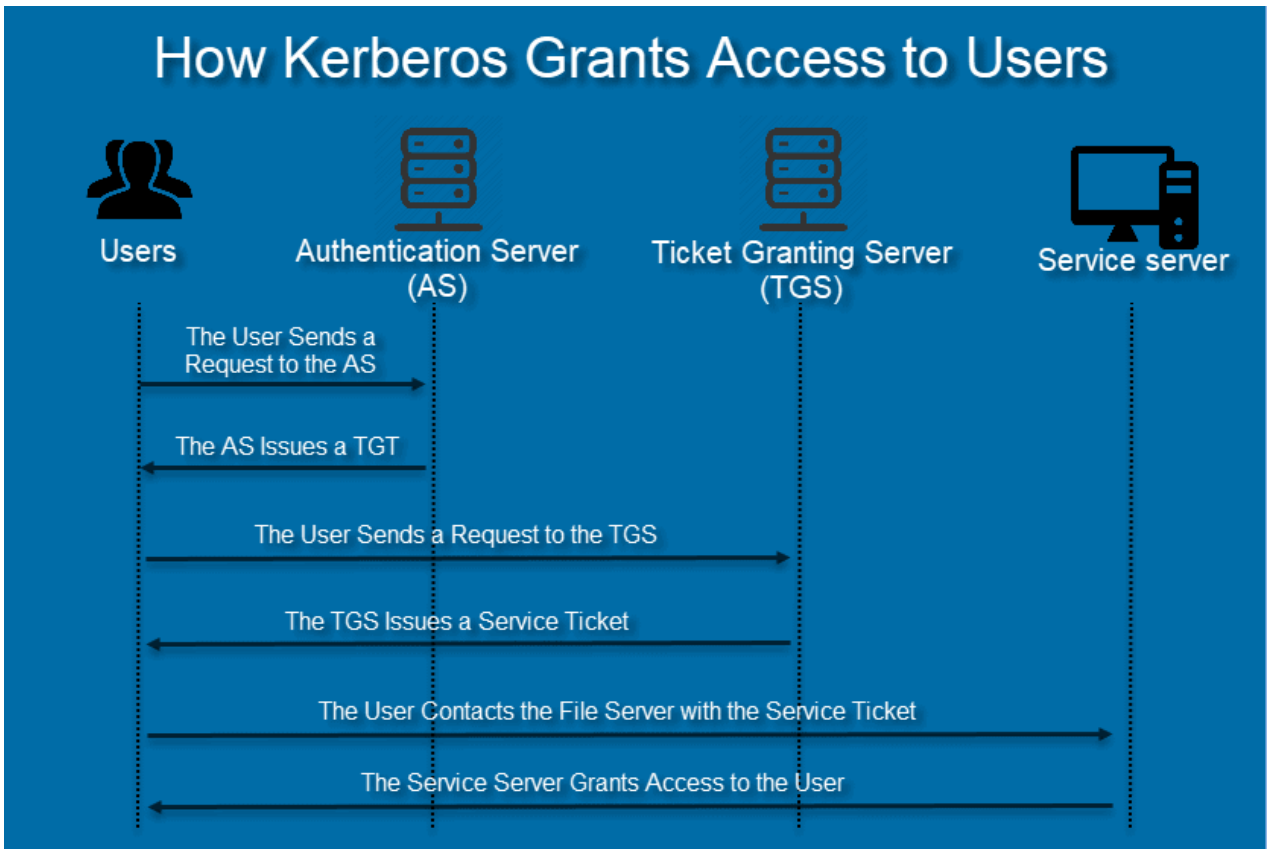


Рисунок 4 – Схема аутентификации Kerberos

Ни одна модель безопасности не является полностью неуязвимой, и Kerberos не является исключением. Поскольку Kerberos так широко используется, у хакеров было достаточно возможностей найти способы обойти его.

Самые большие угрозы для системы Kerberos – это поддельные билеты, повторные попытки угадать пароль и вредоносное ПО, снижающее уровень шифрования. Сочетание всех трех тактик-обычный рецепт успешного прорыва.

К наиболее успешным методам взлома Kerberos относятся:

– *Pass-the-ticket*: злоумышленник подделывает ключ сеанса и представляет поддельные учетные данные для доступа к ресурсам. Хакеры обычно подделывают золотой билет (билет, предоставляющий доступ администратору домена) или серебряный билет (билет, предоставляющий доступ к сервису);
– *Вброс учетных данных и атаки грубой силы*: автоматизированные, продолжающиеся попытки угадать пароль пользователя. Большинство атак грубой силы идут после первоначальной продажи билетов и предоставления услуг по продаже билетов;
– *Вредоносная программа Skeleton key*: эта вредоносная программа обходит Kerberos и понижает уровень шифрования ключей. Для запуска кибератаки злоумышленник должен иметь доступ администратора;

– *Атака DCShadow*: этот взлом происходит, когда злоумышленники получают достаточный доступ в сети, чтобы настроить свой собственный DC для дальнейшего проникновения.

Несмотря на эти опасности, Kerberos остается лучшим протоколом безопасности, доступным сегодня. Если пользователи практикуют правильную политику выбора пароля, вероятность взлома минимальна.

3.2 Kerio Control – комплексная безопасность сети

Kerio Control — это комплексное решение безопасности, которое сочетает в себе несколько функций, включая межсетевой экран и маршрутизатор, систему обнаружения и предотвращения вторжений (IPS), антивирус, VPN и фильтр содержимого. Эти обширные возможности и беспрецедентная гибкость развертывания делают Kerio Control идеальным выбором для малых и средних предприятий.

Прототипом программного пакета Kerio Control был программный шлюз Winroute Pro, первая версия которого была выпущена в 1997 году. Программное обеспечение Winroute Pro представляло собой усовершенствованный прокси-сервер, предназначенный для обеспечения доступа локальным компьютерам в Интернет через единый внешний интернет-канал. Этот продукт практически сразу завоевал популярность и быстро стал конкурентом одного из самых распространенных в то время прокси-серверов Wingate. Уже тогда продукты Kerio отличались понятным интерфейсом и простой настройкой, а также, что немаловажно, надежностью и безопасностью. С тех пор Kerio Winroute постоянно обновлялся, и в него было добавлено множество полезных функций и возможностей. В начале своего пути он назывался Winroute Pro, затем название было изменено на Winroute Firewall, а начиная с 7-й версии продукт получил свое текущее имя – Kerio Control [24].

Установка Kerio Control может быть выполнена либо с помощью Software Appliance, то есть путем развертывания системы из отдельного ISO-образа, либо путем инициализации виртуальной машины на сервере виртуализации. Последний метод включает несколько способов установки, включая возможность автоматической загрузки последней версии Kerio Control с веб-сайта производителя через Vmware VA Marketplace. При установке с ISO-образа все шаги по развертыванию Kerio Control состоят из ответов администратора на несколько простых вопросов мастера установки. Инициализация Kerio Control VM позволяет пропустить основной этап установки, и администратору нужно только установить начальные параметры виртуальной машины: количество процессоров, объем оперативной памяти, количество сетевых адаптеров, размер диска и т.п. В базовой версии Kerio Control VM имеет самые минимальные параметры, но для дальнейшего администрирования необходим хотя бы один сетевой адаптер, указанный в свойствах машины.

Веб-интерфейс управления Kerio Control имеет не только административную панель, но и отдельный пользовательский интерфейс (рисунок 5). Административная панель не имеет возможности что-либо изменить в Kerio Control, но позволяет отслеживать статистику пользователей или пользователя за различные периоды времени. Статистика предоставляет данные о посещенных ресурсах, объеме переданных данных и другую информацию. Если у пользователя есть учетная запись администратора в системе Kerio Control, он также может получать статистику о других пользователях системы через эту панель управления. Точная и продуманная статистика помогает администратору узнать предпочтения пользователей при работе в Интернете, найти критические элементы и проблемы. Панель генерирует подробную гистограмму использования трафика для каждого пользователя в сети. Администратор может выбрать период, за который он хочет отслеживать использование трафика. Кроме того, Kerio Control показывает статистику фактического использования трафика по его типам: HTTP, FTP, электронная почта, потоковые мультимедийные протоколы, обмен данными напрямую между компьютерами или прокси.

В текущее время для предприятия, филиалы которого могут быть расположены в разных городах, безопасное подключение к корпоративной сети является обязательным условием, поскольку сегодня активно развивается аутсорсинг. С Kerio Control настройка виртуальной частной сети практически не требует усилий. Сервер и клиенты VPN являются неотъемлемой частью возможностей безопасного удаленного доступа Kerio Control к корпоративной сети. Использование виртуальной сети Kerio VPN позволяет пользователям удаленно подключаться к любым ресурсам корпоративной сети и работать с сетью организации, как если бы это была их собственная локальная сеть.

Встроенный сервер Kerio Control VPN позволяет организовать сети VPN по двум различным сценариям: «сервер-сервер» и «клиент-сервер» (используется Kerio VPN Client для Windows, Mac и Linux). Режим «сервер-сервер» используется предприятиями, которые хотят подключить удаленный офис через безопасный канал для совместного использования общих ресурсов. Этот сценарий требует наличия Kerio Control на каждой из подключающихся сторон, чтобы установить безопасный канал через открытый Интернет. Режим «клиент-сервер» позволяет удаленному пользователю безопасно подключить портативный или домашний компьютер к корпоративной сети. Как известно многим системным администраторам, протоколы VPN и NAT (трансляция сетевых адресов) не всегда поддерживают совместную работу. Решение Kerio VPN предназначено для надежной работы через NAT и даже через несколько шлюзов NAT. Kerio VPN использует стандартные алгоритмы шифрования SSL для управления каналами (TCP) и Blowfish для передачи данных (UDP) и поддерживает IPsec.

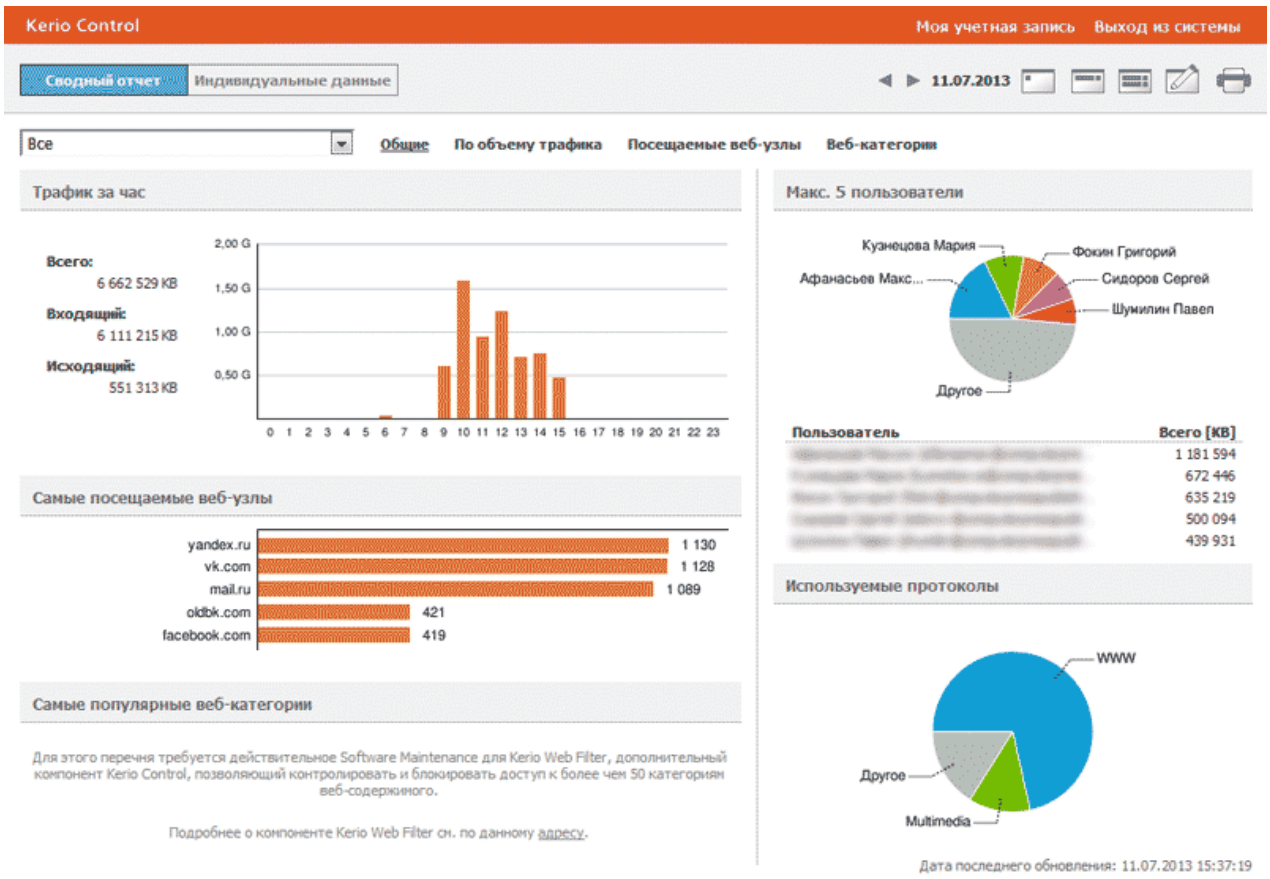


Рисунок 5 – Панель пользователя

Шлюз Kerio Control имеет встроенную защиту от вирусов, которая обеспечивается проверкой как входящего, так и исходящего трафика. Если ранее в Kerio Control использовался встроенный антивирус от McAfee, то в последних версиях используется антивирус Sophos. Администратор может установить правила проверки для трафика по различным протоколам: SMTP и POP3, WEB (HTTP) и пересылка файлов (FTP). Встроенный антивирус межсетевого экрана, установленный на шлюзе, обеспечивает полную защиту трафика, проходящего через шлюз. Поскольку встроенный антивирус может получать обновления с новыми вирусными базами в режиме реального времени, это значительно повышает уровень сетевой безопасности, а также позволяет использовать антивирусные программы на каждом компьютере в локальной сети. Антивирус проверяет входящие и исходящие сообщения, а также все вложения. Если во вложении обнаруживается вирус, все вложения удаляются, а к сообщению добавляется уведомление. Кроме того, Kerio Control проверяет весь сетевой трафик, включая HTML-страницы, на наличие встроенных вирусов. Файлы, загружаемые по HTTP, и файлы, передаваемые по FTP, также проверяются на вирусы. Кроме того, следует отметить, что для организаций и учреждений, таких как школы, которые не хотят, чтобы их сотрудники и клиенты посещали определенные страницы, Kerio Control со встроенным веб-фильтром Kerio Control (доступным в качестве опции за

дополнительную плату) предоставляет дополнительные возможности блокировки страниц в Интернете.

Kerio Control позволяет администраторам не только создавать общую стратегию использования трафика, но также устанавливать и применять ограничения для каждого пользователя. Прежде чем получить доступ в Интернет, каждый пользователь должен войти в Kerio Control. Учетные записи пользователей хранятся в отдельной внутренней базе данных пользователей или берутся из корпоративной базы данных Microsoft Active Directory или Apple Open Directory. Возможно параллельное использование как локальных, так и доменных пользовательских баз данных. В случае интеграции с Microsoft Active Directory авторизация клиента может происходить прозрачно для пользователей домена через аутентификацию NTLM. В составе Windows 2008/2012 Server Active Directory позволяет администраторам централизованно управлять учетными записями пользователей и данными сетевых ресурсов. Active Directory обеспечивает доступ к пользовательской информации с одного компьютера. Поддержка Active Directory / Open Directory обеспечивает Kerio Control доступ в реальном времени к базе данных пользователей и позволяет установить пользователя в локальной сети без сохранения пароля. Таким образом, вам не нужно синхронизировать пароли для каждого пользователя. Все изменения в Microsoft Active Directory / Open Directory автоматически отражаются в Kerio Control.

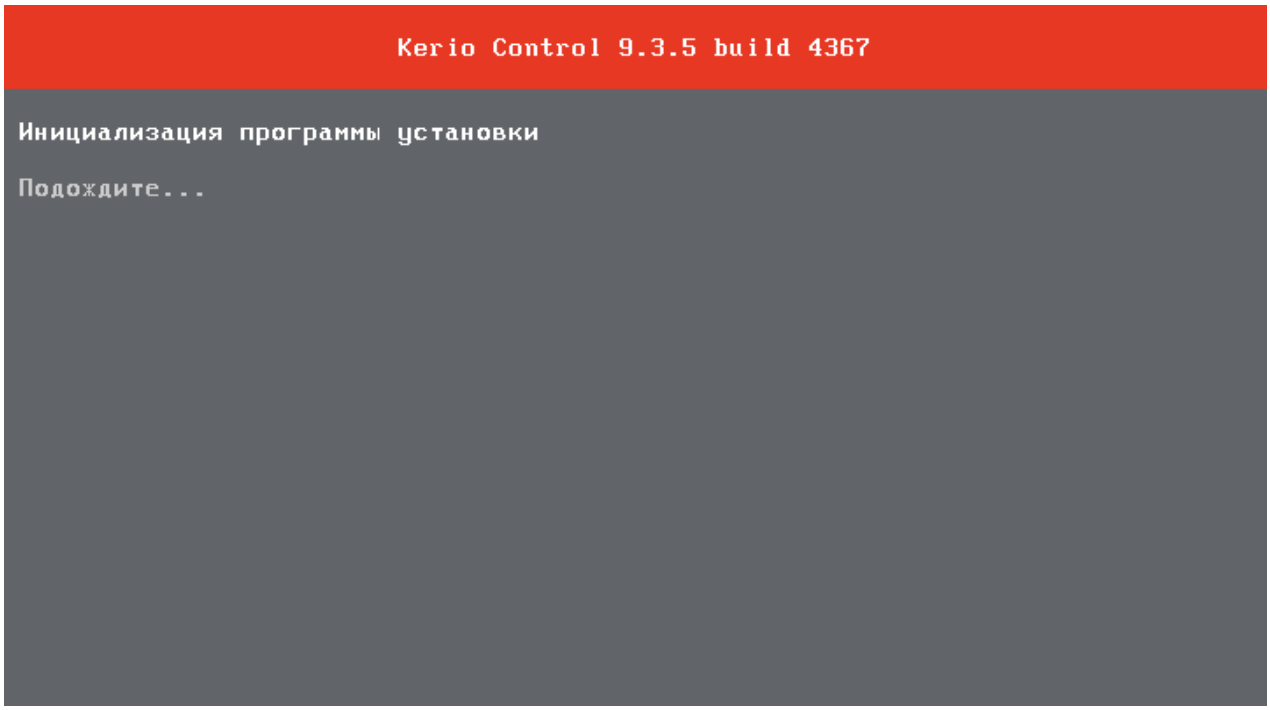
Администратор может установить разные ограничения доступа для каждого пользователя. Действие этих правил можно устанавливать на определенные периоды времени и устанавливать различные ограничения на использование трафика. Когда лимит достигнут, Kerio Control отправляет по электронной почте предупреждение пользователю и администратору, или администратор блокирует этого пользователя до конца дня или месяца.

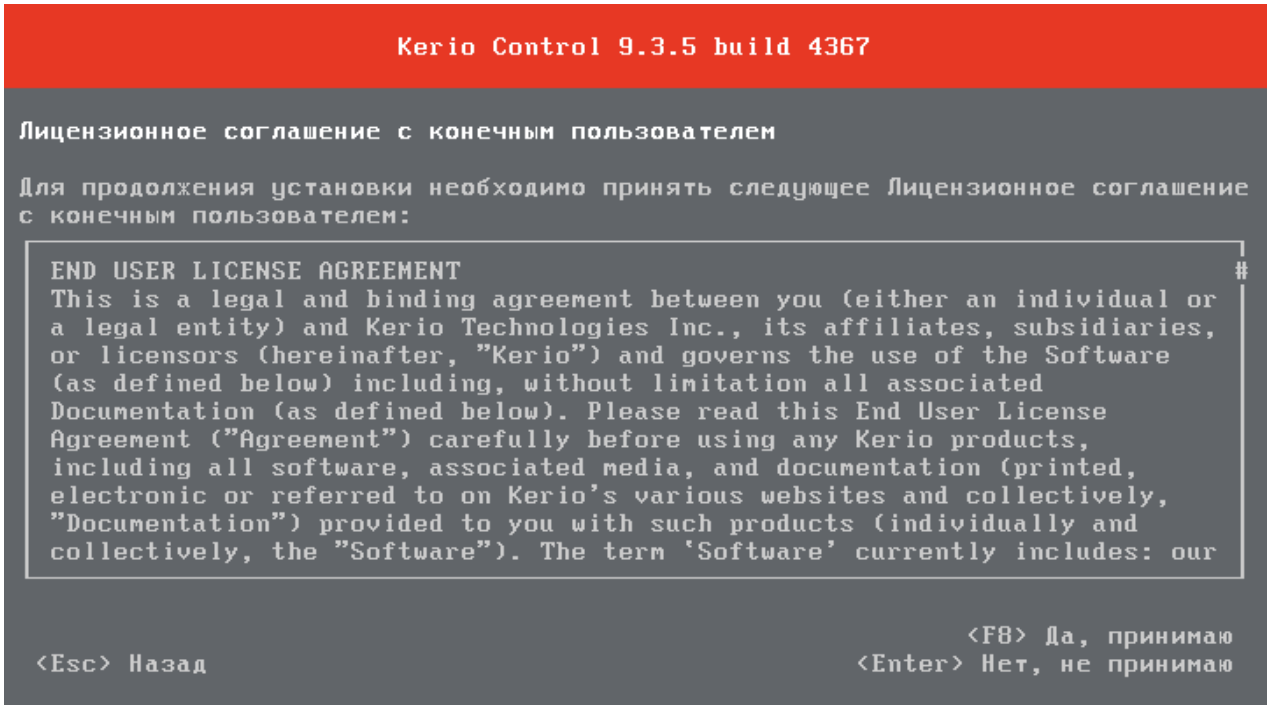
3.3 Развертывание Kerio Control

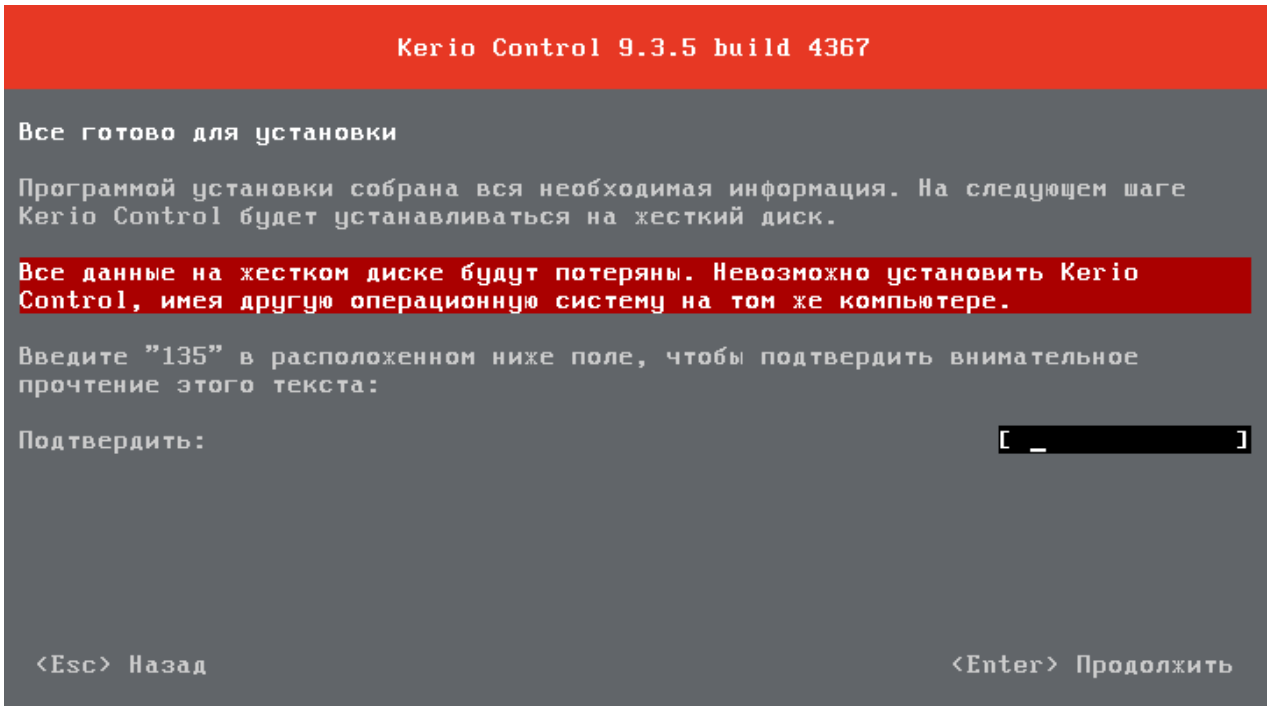
В данном разделе мы приведем алгоритм установки и настройки Kerio Control на практике:

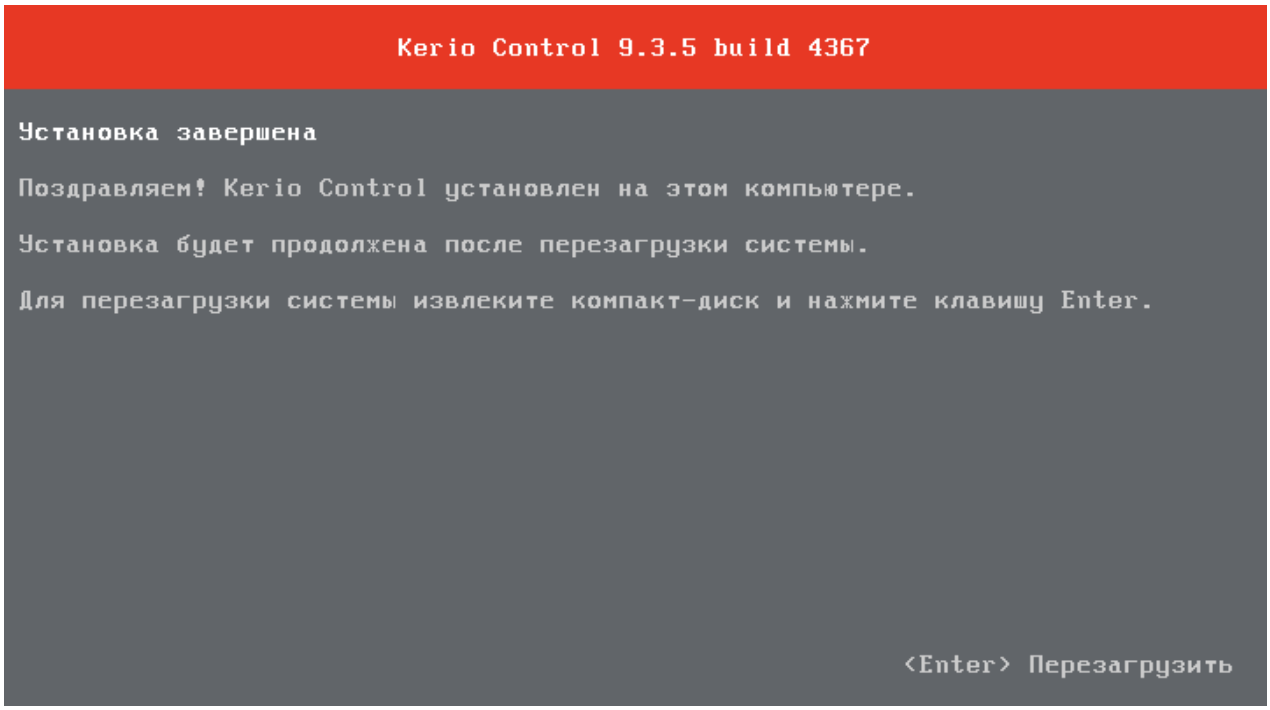
Шаг 1. Подключить образ диска в дисковод и запустить установку.


Kerio Control 9.3.5 build 4367
Please select installation language:
Français
Hrvatski
Magyar
Italiano
Nederlands
Polski
Português
Русский
<Enter> Continue

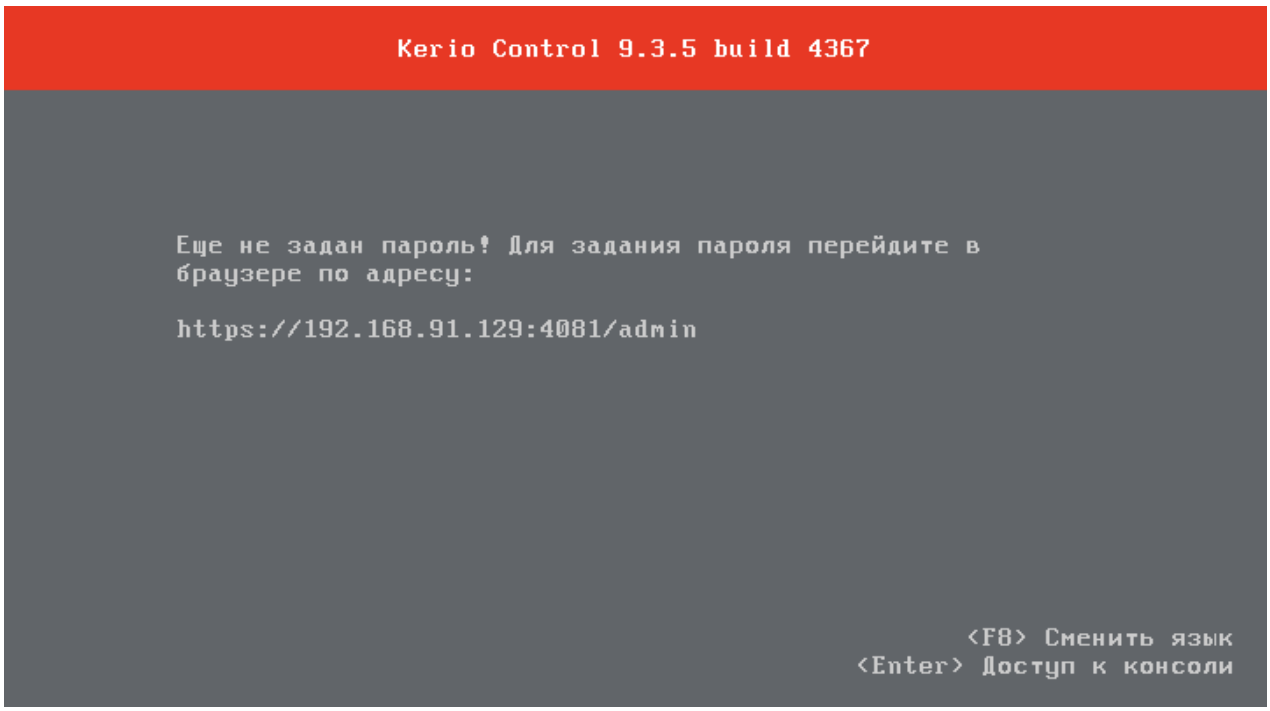

Kerio Control 9.3.5 build 4367
Инициализация программы установки
Подождите...


Kerio Control 9.3.5 build 4367
Лицензионное соглашение с конечным пользователем
Для продолжения установки необходимо принять следующее Лицензионное соглашение с конечным пользователем:
END USER LICENSE AGREEMENT
This is a legal and binding agreement between you (either an individual or a legal entity) and Kerio Technologies Inc., its affiliates, subsidiaries, or licensors (hereinafter, "Kerio") and governs the use of the Software (as defined below) including, without limitation all associated Documentation (as defined below). Please read this End User License Agreement ("Agreement") carefully before using any Kerio products, including all software, associated media, and documentation (printed, electronic or referred to on Kerio's various websites and collectively, "Documentation") provided to you with such products (individually and collectively, the "Software"). The term 'Software' currently includes: our
<F8> Да, принимаю
<Esc> Назад
<Enter> Нет, не принимаю

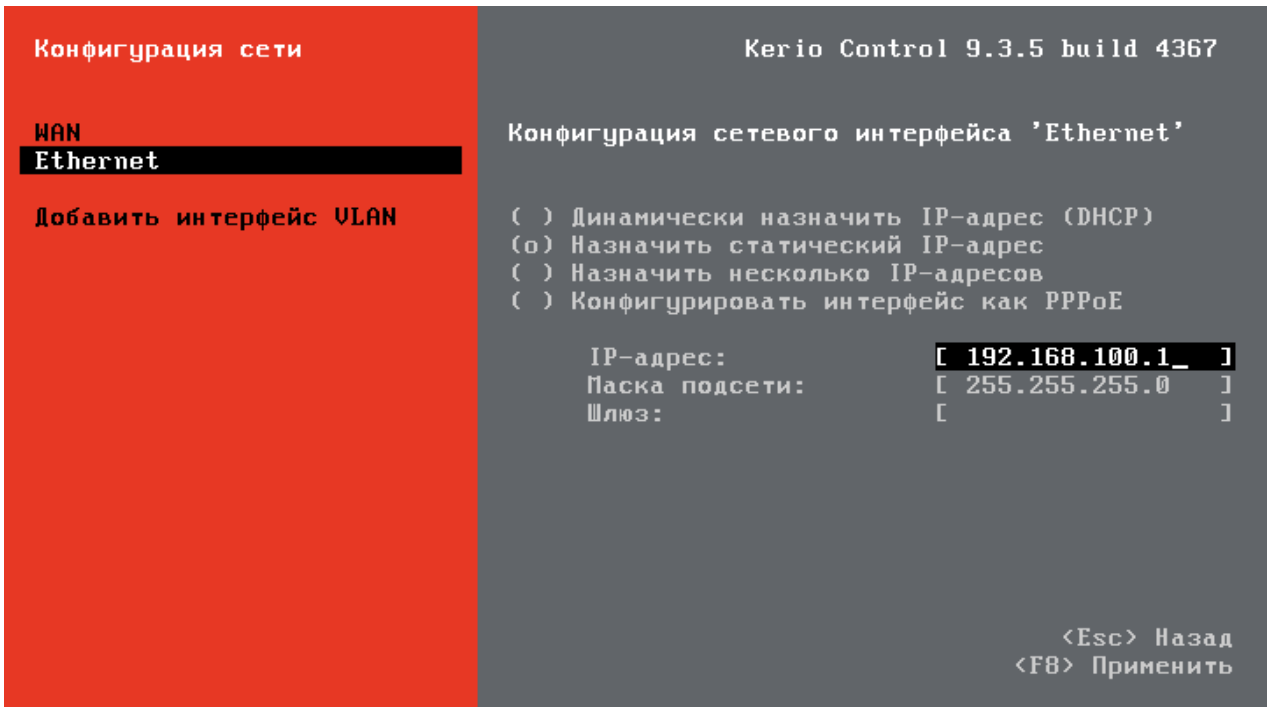

Kerio Control 9.3.5 build 4367
Все готово для установки
Программой установки собрана вся необходимая информация. На следующем шаге Kerio Control будет устанавливаться на жесткий диск.
Все данные на жестком диске будут потеряны. Невозможно установить Kerio Control, имея другую операционную систему на том же компьютере.
Введите "135" в расположенном ниже поле, чтобы подтвердить внимательное прочтение этого текста:
Подтвердить:
[_]
<Esc> Назад
<Enter> Продолжить

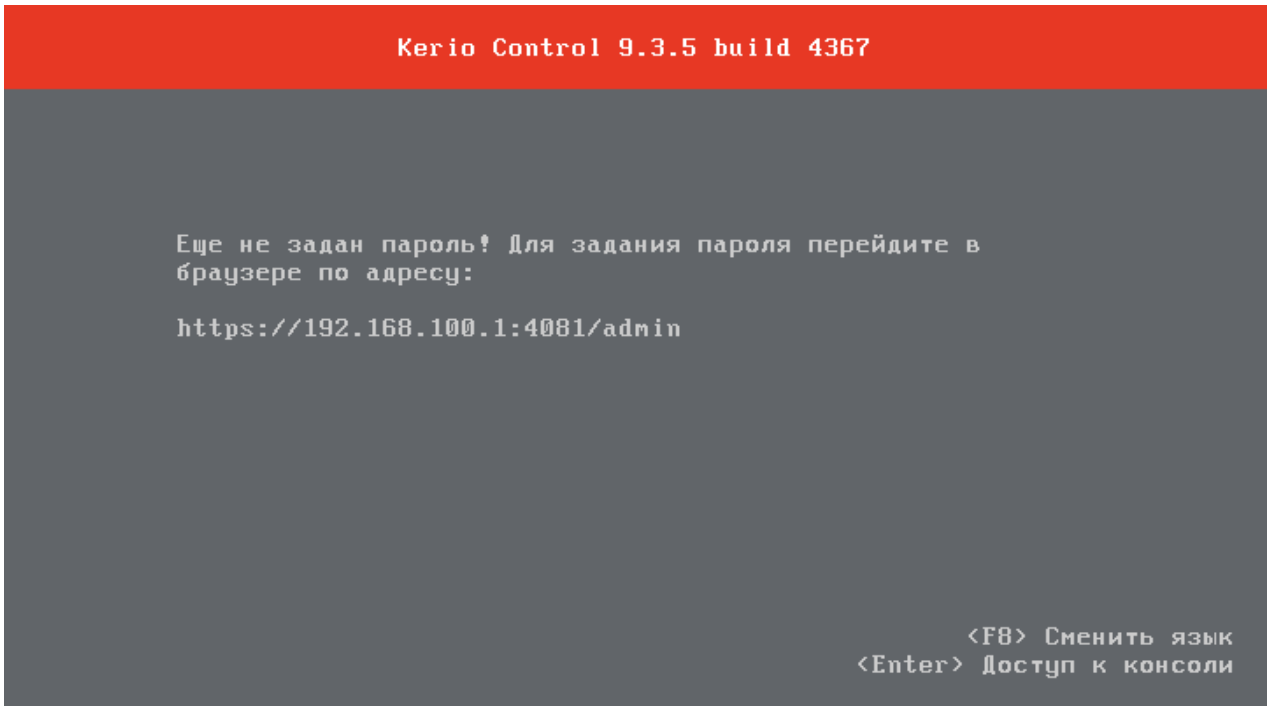


Шаг 2. Изменить автоматически сгенерированный IP адрес на IP адрес вашей сети. Задать пароль администратора через Web браузер по адресу, указанному системой.

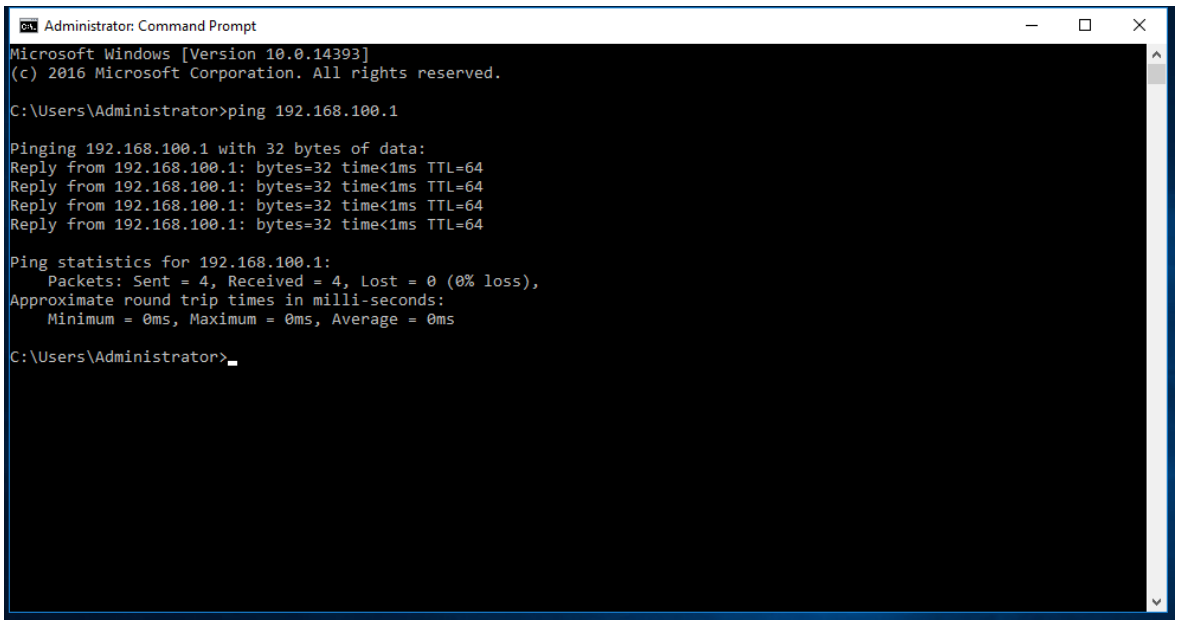

Kerio Control 9.3.5 build 4367
Еще не задан пароль! Для задания пароля перейдите в браузере по адресу:
https://192.168.91.129:4081/admin
<F8> Сменить язык
<Enter> Доступ к консоли


Kerio Control 9.3.5 build 4367
Конфигурация сети
Удаленное администрирование
Завершить работу
Перезапустить
Заводские настройки
Выберите этот пункт для просмотра или изменения основной конфигурации сети, если невозможно использовать удаленное администрирование.
<Вверх/вниз> Переместить
<Enter> Выбрать
<Esc> Назад

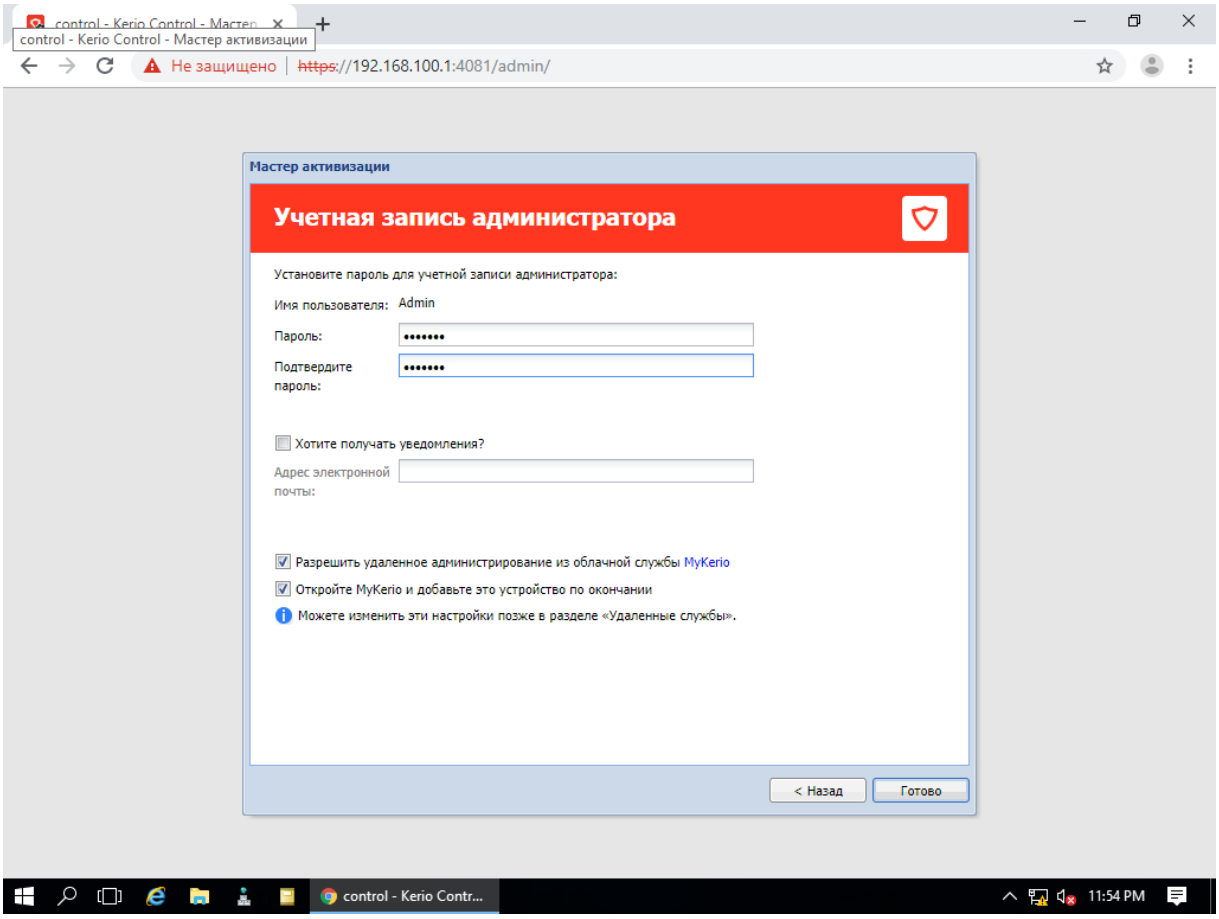


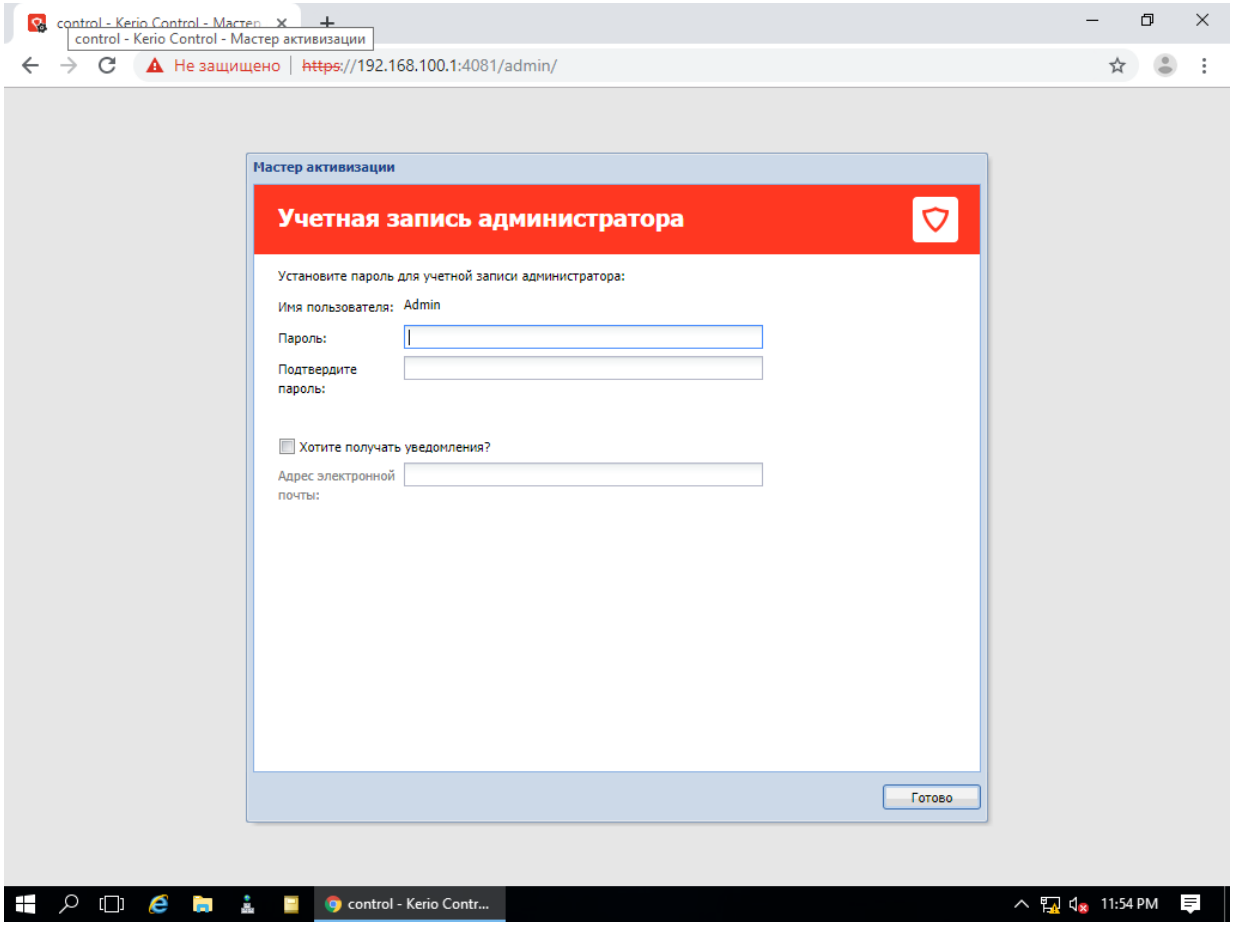


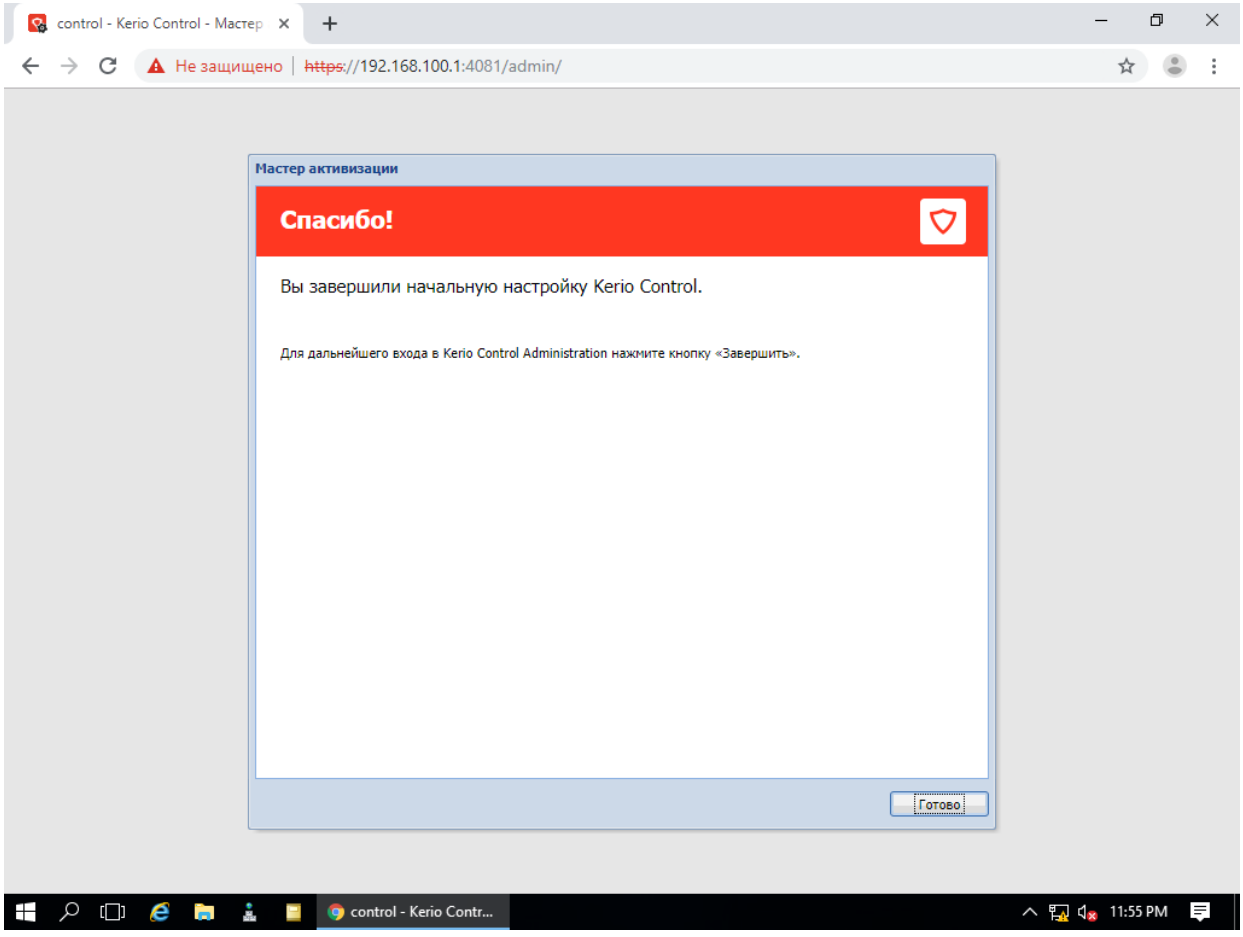
Шаг 3. Проверить доступность сервиса при помощи утилиты ping.

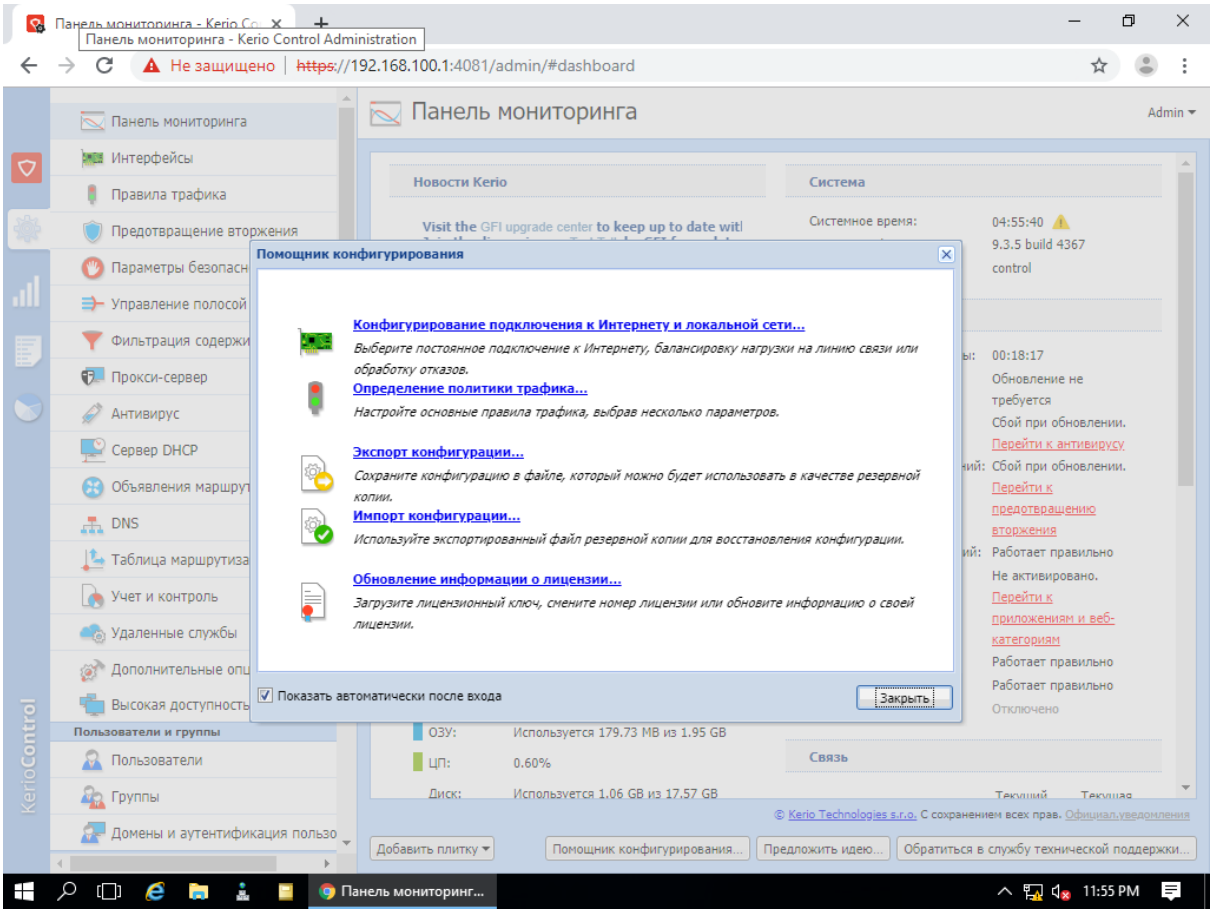


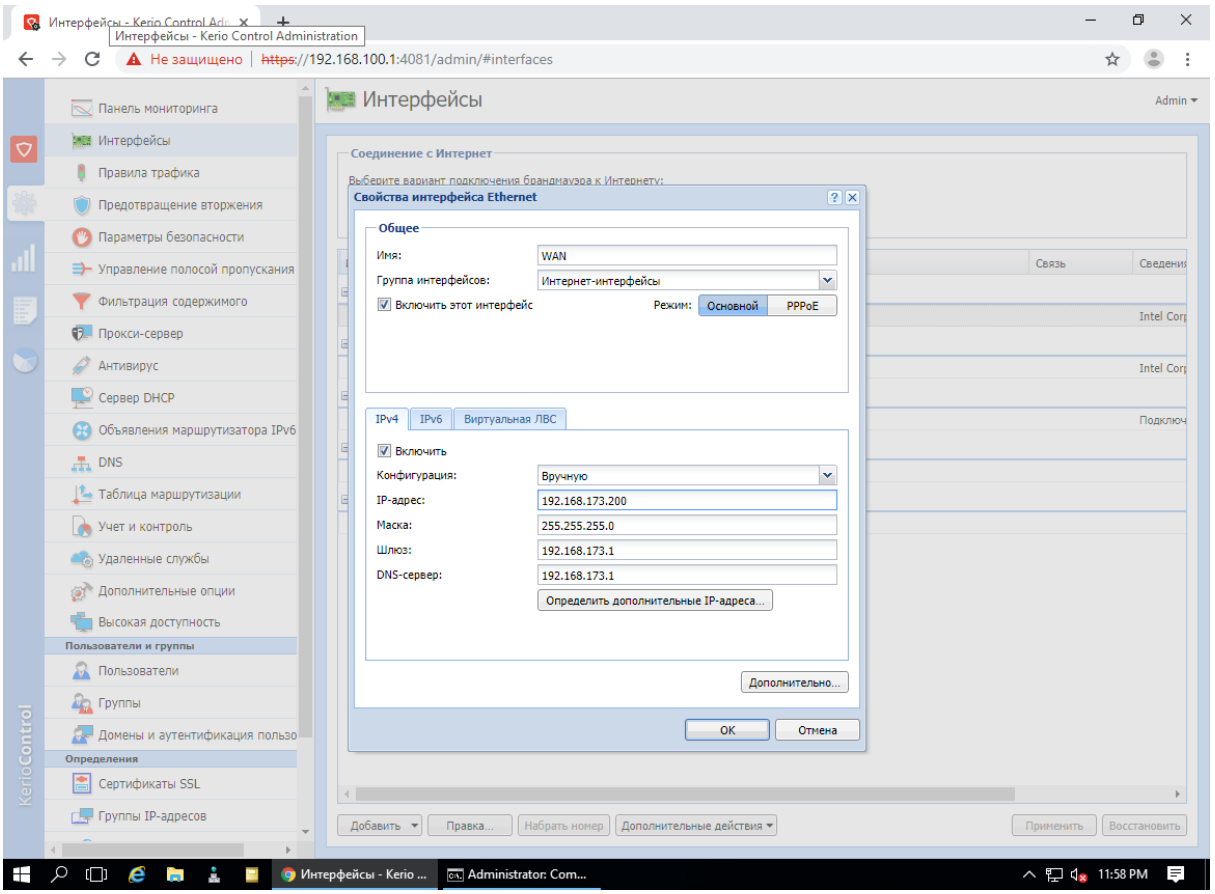
Шаг 4. Настройте параметры системы и интерфейсов.



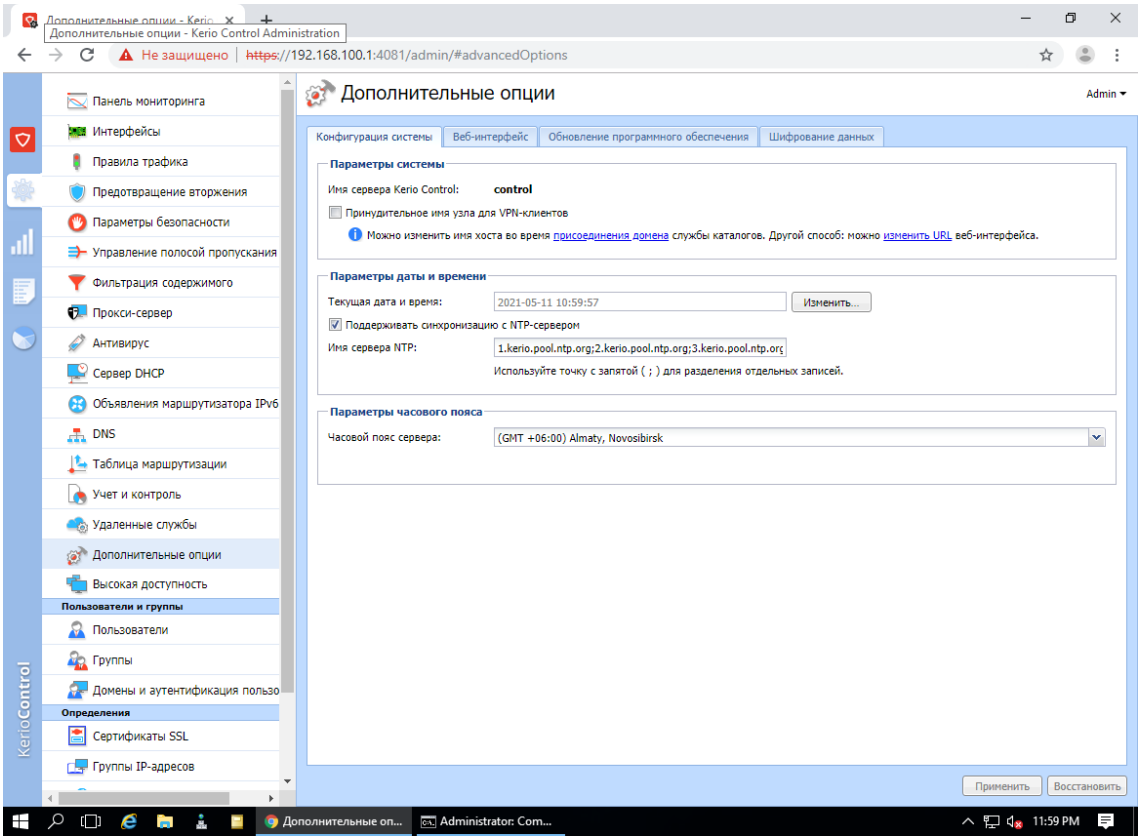

control - Kerio Control - Мастер активизации
Не защищено | https://192.168.100.1:4081/admin/
Мастер активизации
Учетная запись администратора
Установите пароль для учетной записи администратора:
Имя пользователя: Admin
Пароль:
Подтвердите пароль:
Хотите получать уведомления?
Адрес электронной почты:
Готово
control - Kerio Contr...
11:54 PM

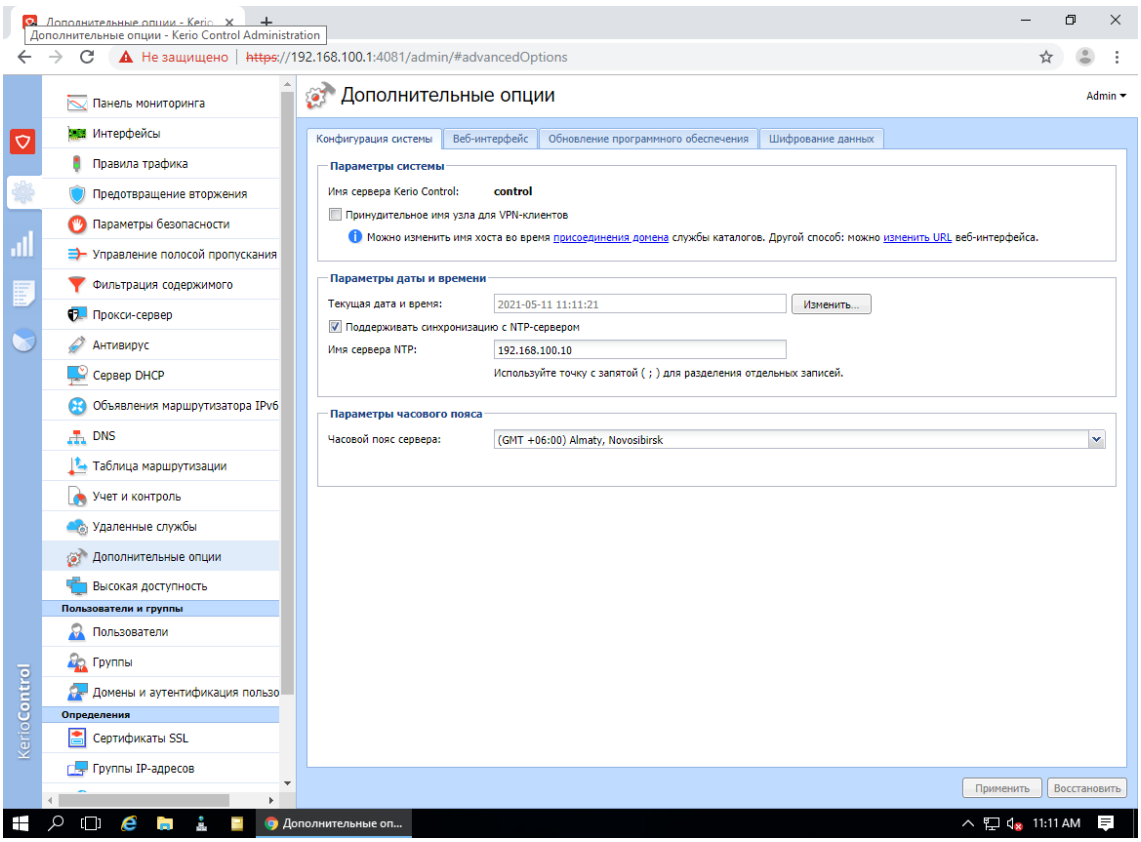

control - Kerio Control - Мастер
Не защищено | https://192.168.100.1:4081/admin/
Мастер активизации
Спасибо!
Вы завершили начальную настройку Kerio Control.
Для дальнейшего входа в Kerio Control Administration нажмите кнопку «Завершить».
Готово
control - Kerio Contr...
11:55 PM


Панель мониторинга - Kerio Control Administration
Не защищено | https://192.168.100.1:4081/admin/#dashboard
Панель мониторинга
Admin
Помощник конфигурирования
Конфигурирование подключения к Интернету и локальной сети...
Выберите постоянное подключение к Интернету, балансировку нагрузки на линию связи или обработку отказов.
Определение политики трафика...
Настройте основные правила трафика, выбрав несколько параметров.
Экспорт конфигурации...
Сохраните конфигурацию в файле, который можно будет использовать в качестве резервной копии.
Импорт конфигурации...
Используйте экспортированный файл резервной копии для восстановления конфигурации.
Обновление информации о лицензии...
Загрузите лицензионный ключ, смените номер лицензии или обновите информацию о своей лицензии.
Показать автоматически после входа
Закрыть
Новости Kerio
Система
Связь
Добавить плитку
Помощник конфигурирования...
Предложить идею...
Обратиться в службу технической поддержки...
11:55 PM

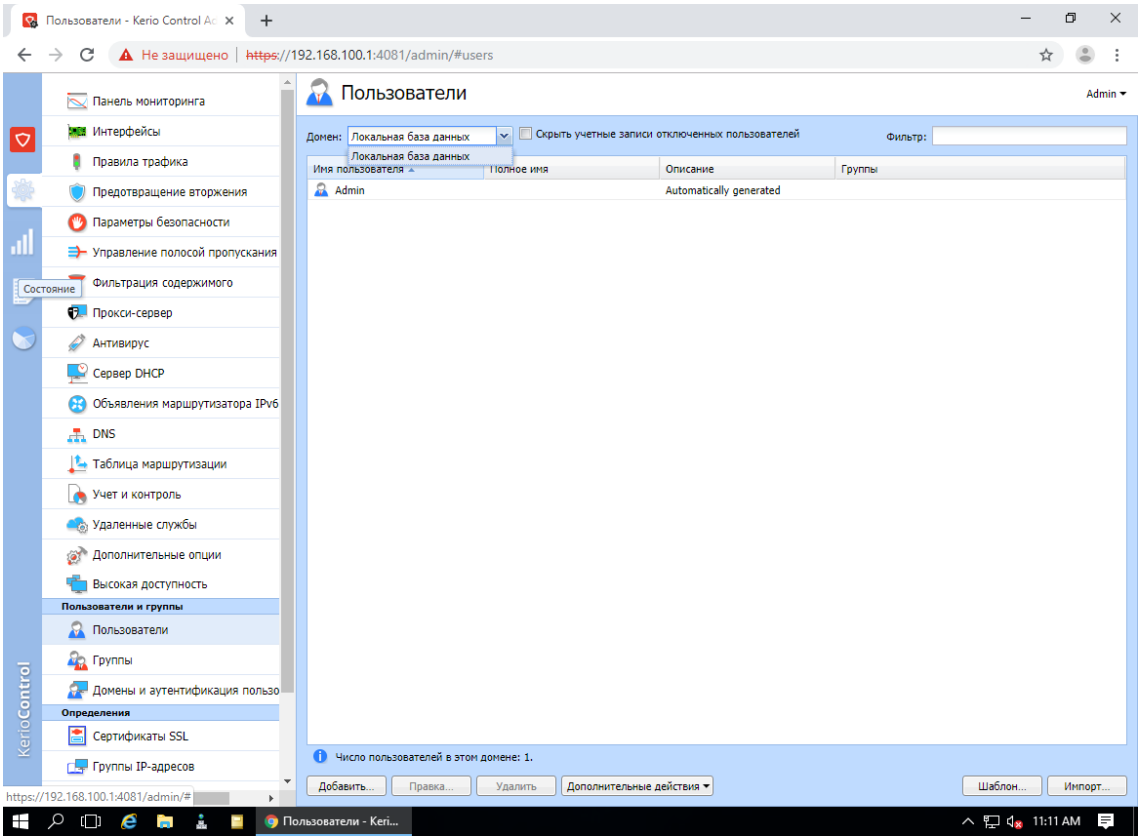

Интерфейсы - Kerio Control Administration
Не защищено | https://192.168.100.1:4081/admin/#interfaces
Интерфейсы
Admin
Соединение с Интернет
Свойства интерфейса Ethernet
Общее
Имя: WAN
Группа интерфейсов: Интернет-интерфейсы
Включить этот интерфейс
Режим: Основной PPPoE
IPv4 IPv6 Виртуальная ЛВС
Включить
Конфигурация: Вручную
IP-адрес: 192.168.173.200
Маска: 255.255.255.0
Шлюз: 192.168.173.1
DNS-сервер: 192.168.173.1
Определить дополнительные IP-адреса...
Дополнительно...
OK
Отмена
Добавить
Правка...
Набрать номер
Дополнительные действия
Применить
Восстановить
11:58 PM

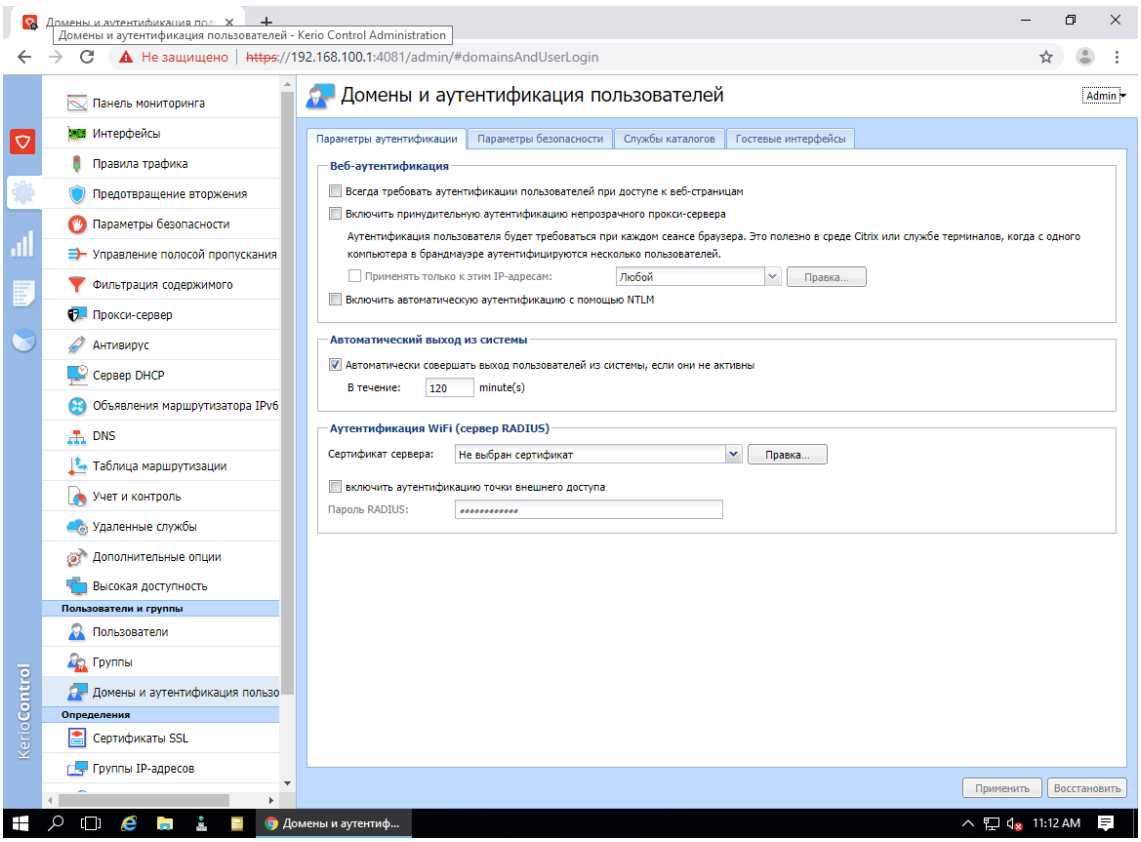
Шаг 5. Синхронизируйте время в Active Directory, т. к. протокол Kerberos очень чувствителен к данному параметру.

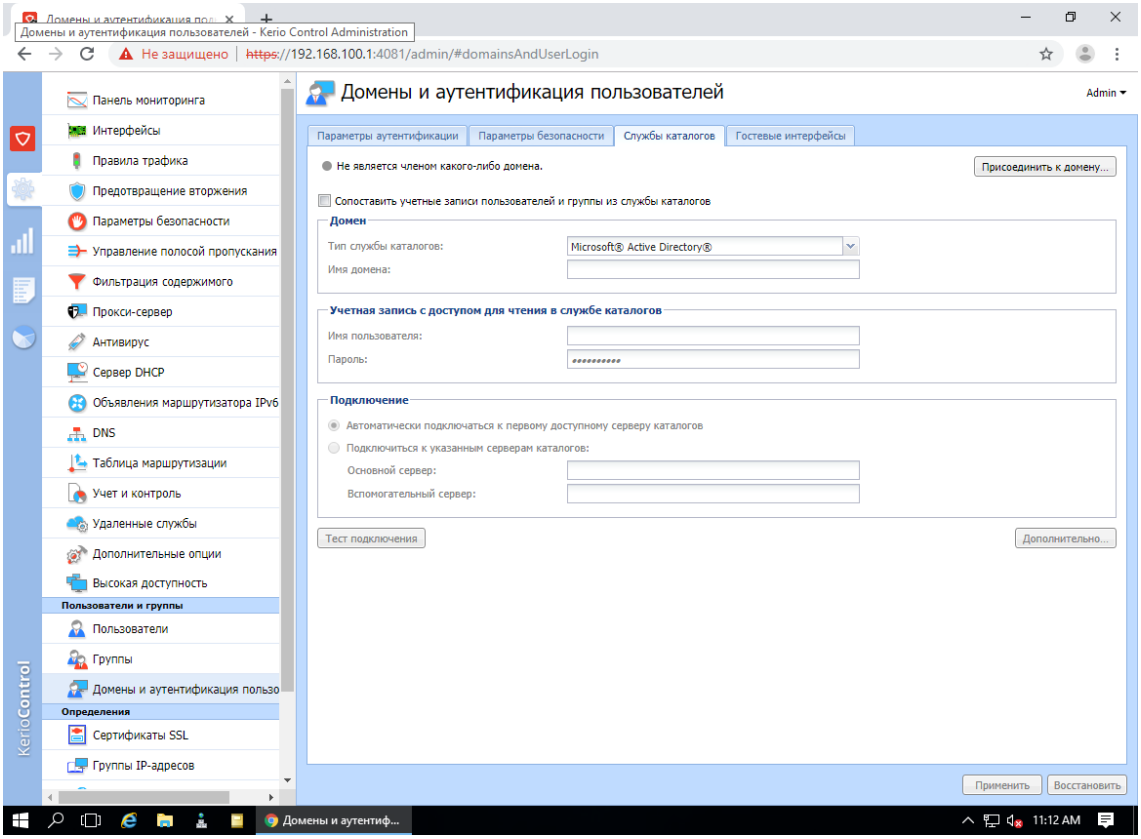


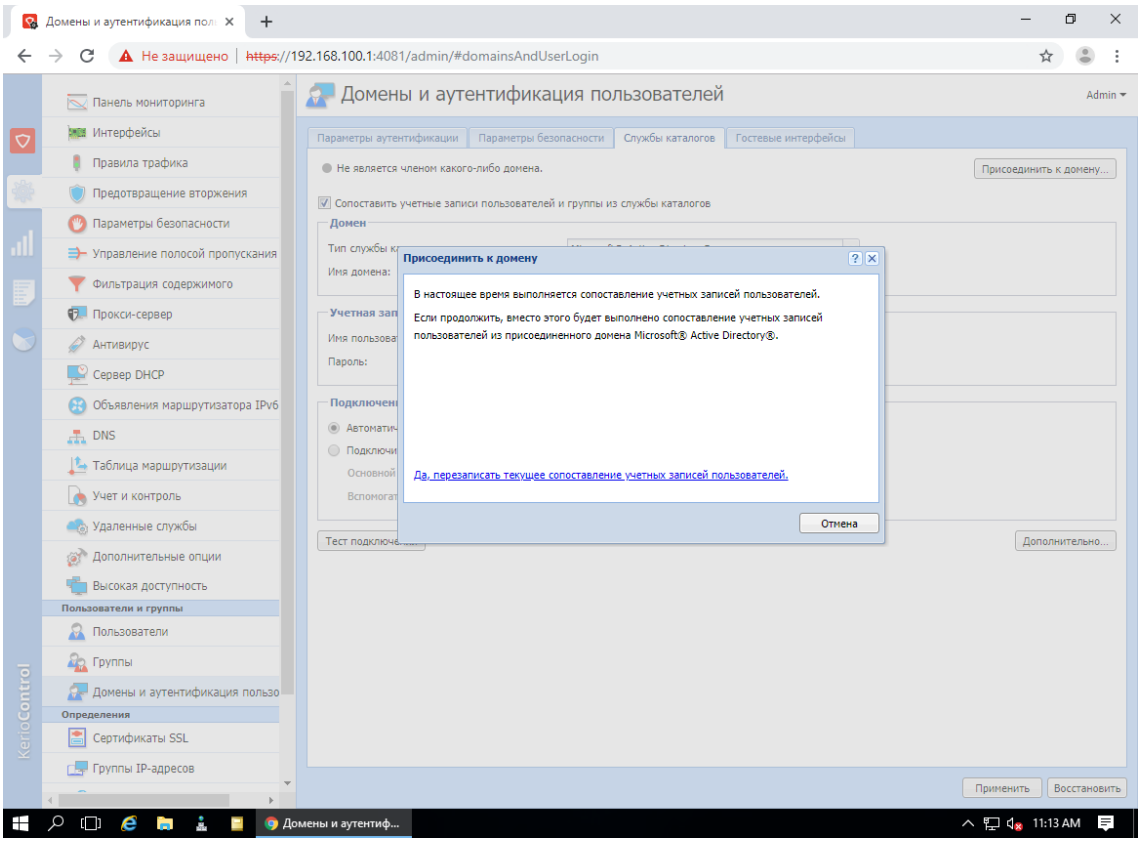


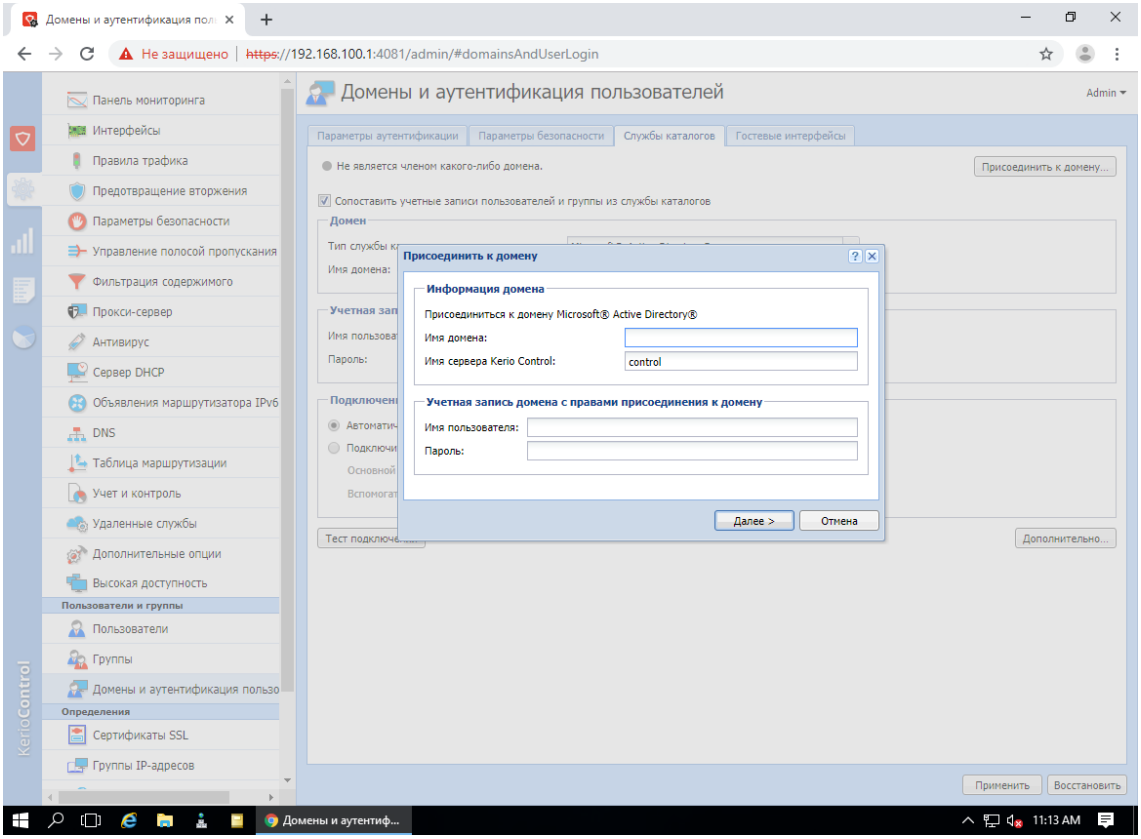
Шаг 6. Подключитесь к домену, чтобы база пользователей синхронизировалась с Kerio Control.

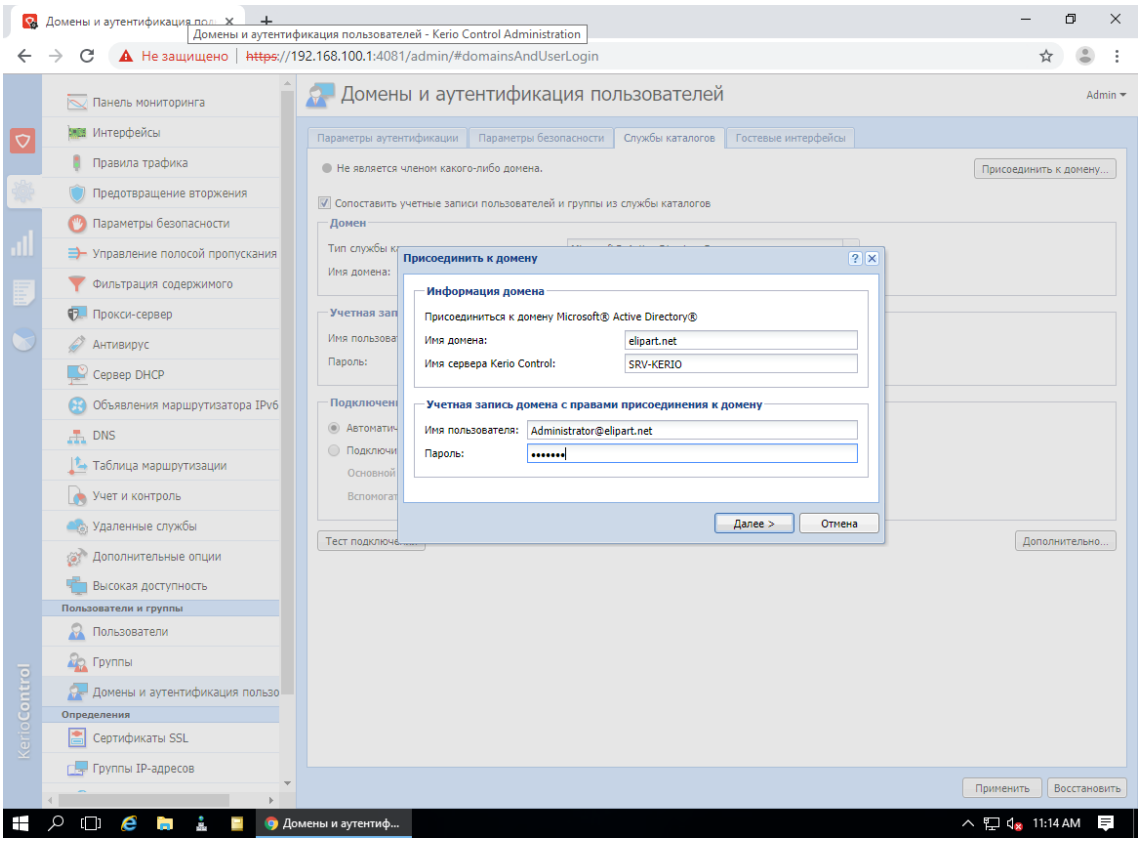


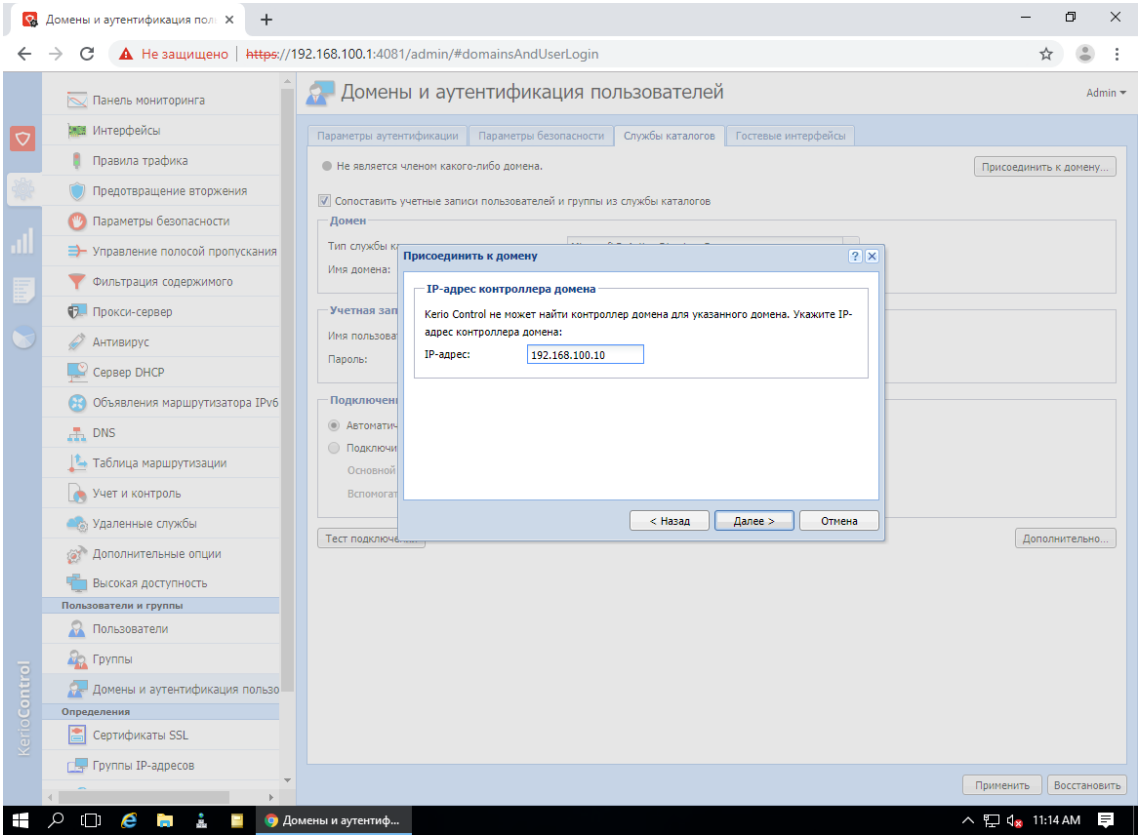


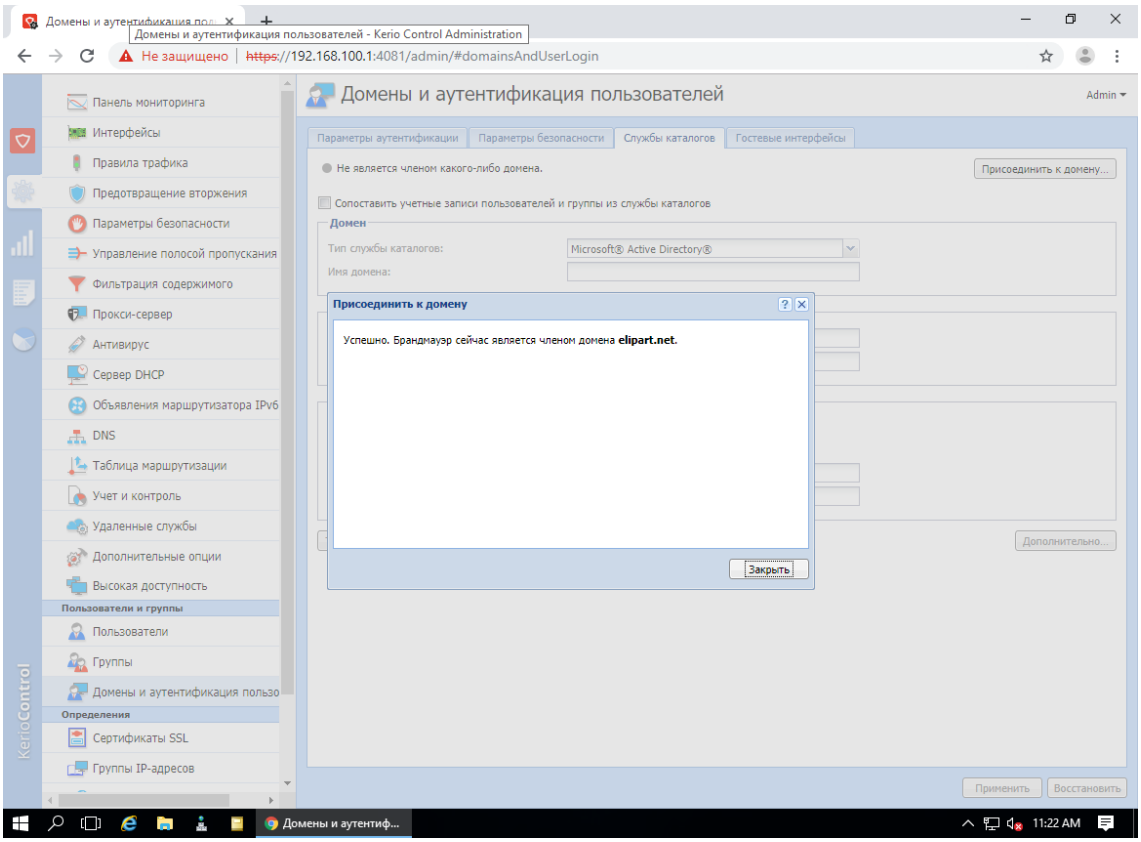

Домены и аутентификация пользователей - Kerio Control Administration
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Не является членом какого-либо домена.
Присоединить к домену...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы каталогов:
Microsoft® Active Directory®
Имя домена:
Учетная запись с доступом для чтения в службе каталогов
Имя пользователя:
Пароль:
Подключение
Автоматически подключаться к первому доступному серверу каталогов
Подключиться к указанным серверам каталогов:
Основной сервер:
Вспомогательный сервер:
Тест подключения
Дополнительно...
Применить
Восстановить
Домены и аутентиф...
11:12 AM

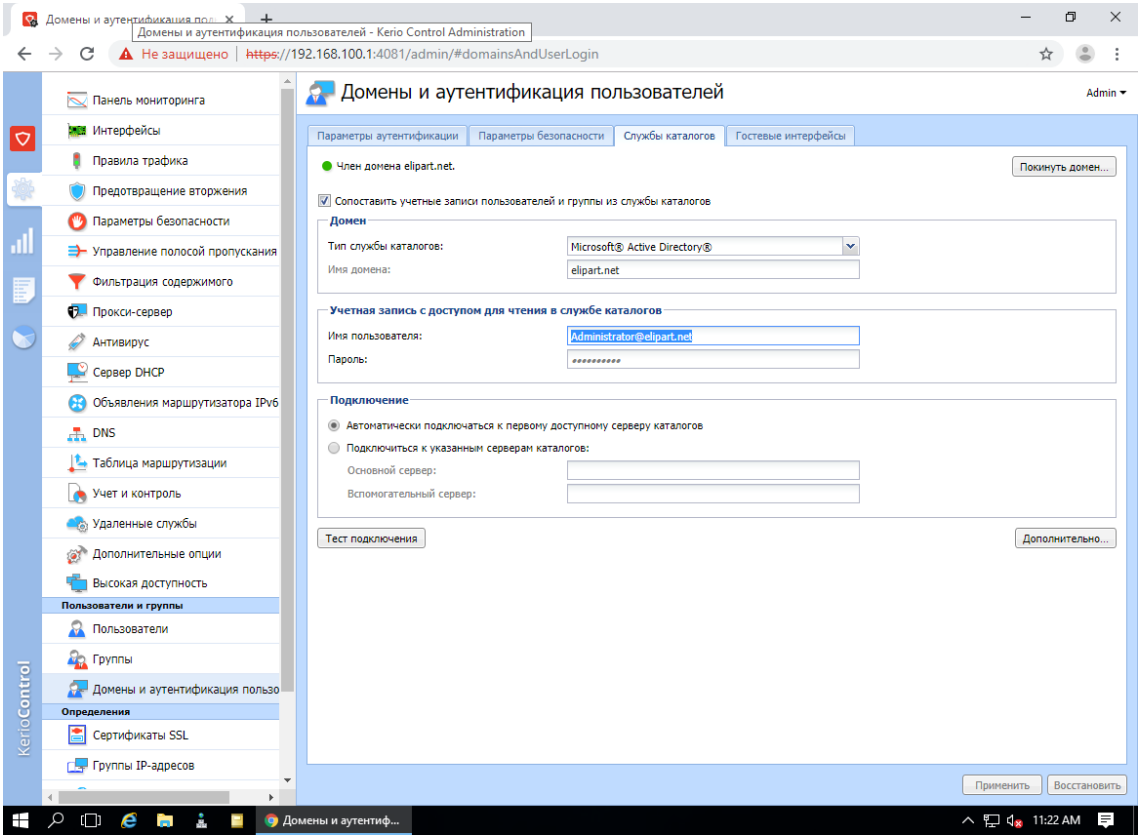

Домены и аутентификация пол
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Присоединить к домену
В настоящее время выполняется сопоставление учетных записей пользователей.
Если продолжить, вместо этого будет выполнено сопоставление учетных записей пользователей из присоединенного домена Microsoft® Active Directory®.
Да, перезаписать текущее сопоставление учетных записей пользователей.
Отмена
Домены и аутентиф...
11:13 AM

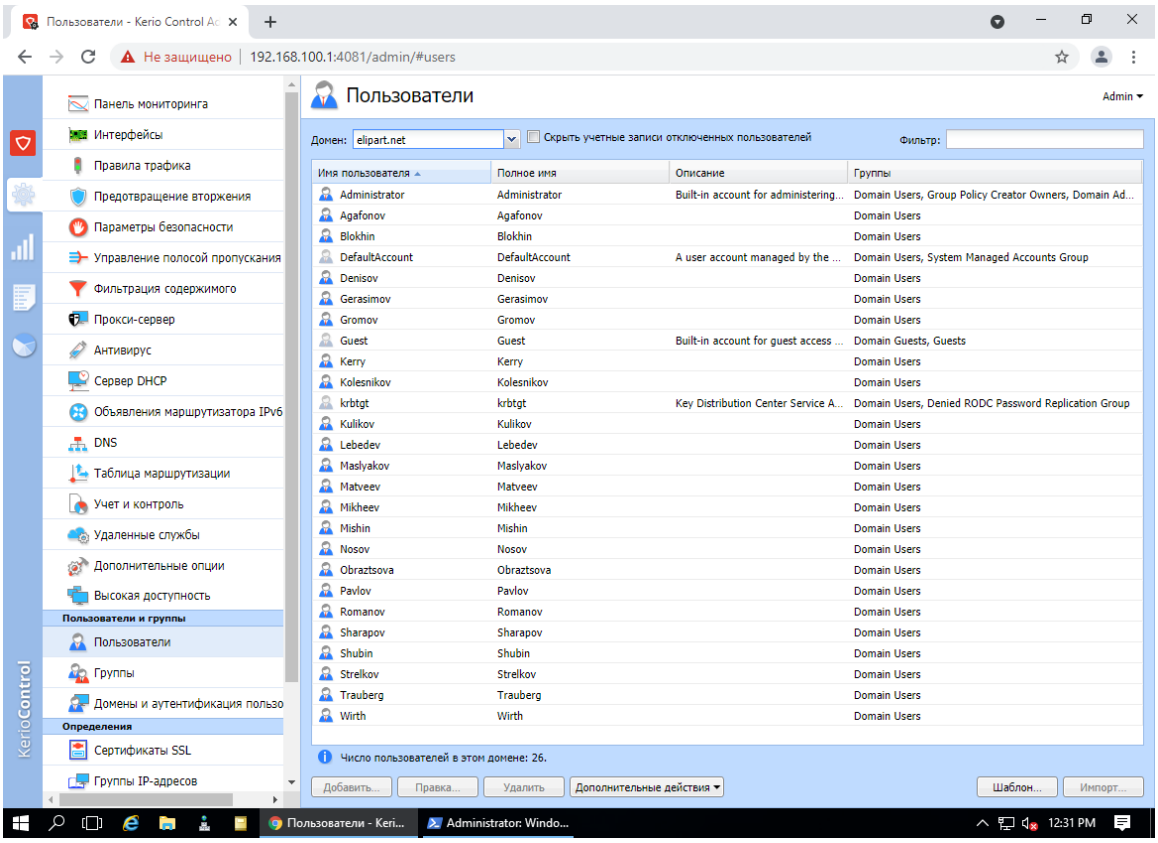

Домены и аутентификация пол
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Не является членом какого-либо домена.
Присоединить к домену...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы
Имя домена:
Учетная зап
Имя пользова
Пароль:
Подключени
Автоматич
Подключи
Основной
Вспомогат
Тест подключе
Дополнительно...
Применить
Восстановить
Присоединить к домену
Информация домена
Присоединиться к домену Microsoft® Active Directory®
Имя домена:
Имя сервера Kerio Control:
control
Учетная запись домена с правами присоединения к домену
Имя пользователя:
Пароль:
Далее >
Отмена
Домены и аутентиф...
11:13 AM


Домены и аутентификация пользователей - Kerio Control Administration
Домены и аутентификация пол
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Не является членом какого-либо домена.
Присоединить к домену...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы
Имя домена:
Учетная зап
Имя пользова
Пароль:
Подключени
Автоматич
Подключи
Основной
Вспомогат
Тест подключе
Дополнительно...
Применить
Восстановить
Присоединить к домену
Информация домена
Присоединиться к домену Microsoft® Active Directory®
Имя домена:
elipart.net
Имя сервера Kerio Control:
SRV-KERIO
Учетная запись домена с правами присоединения к домену
Имя пользователя:
Administrator@elipart.net
Пароль:
Далее >
Отмена
Домены и аутентиф...
11:14 AM

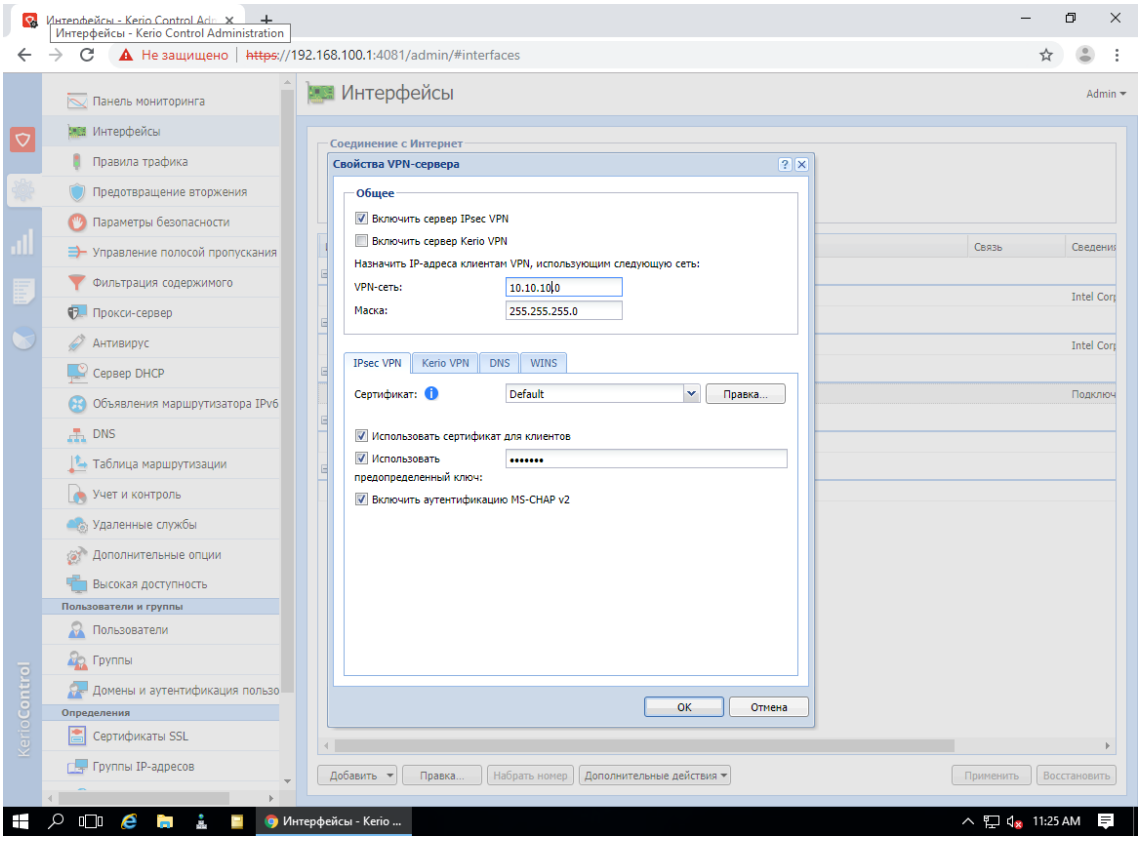

Домены и аутентификация пол
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Не является членом какого-либо домена.
Присоединить к домену...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы к
Имя домена:
Учетная зап
Имя пользова
Пароль:
Подключени
Автоматич
Подключи
Основной
Вспомогат
Тест подключе
Дополнительно...
Применить
Восстановить
Присоединить к домену
IP-адрес контроллера домена
Kerio Control не может найти контроллер домена для указанного домена. Укажите IP-адрес контроллера домена:
IP-адрес:
192.168.100.10
< Назад
Далее >
Отмена
Домены и аутентиф...
11:14 AM

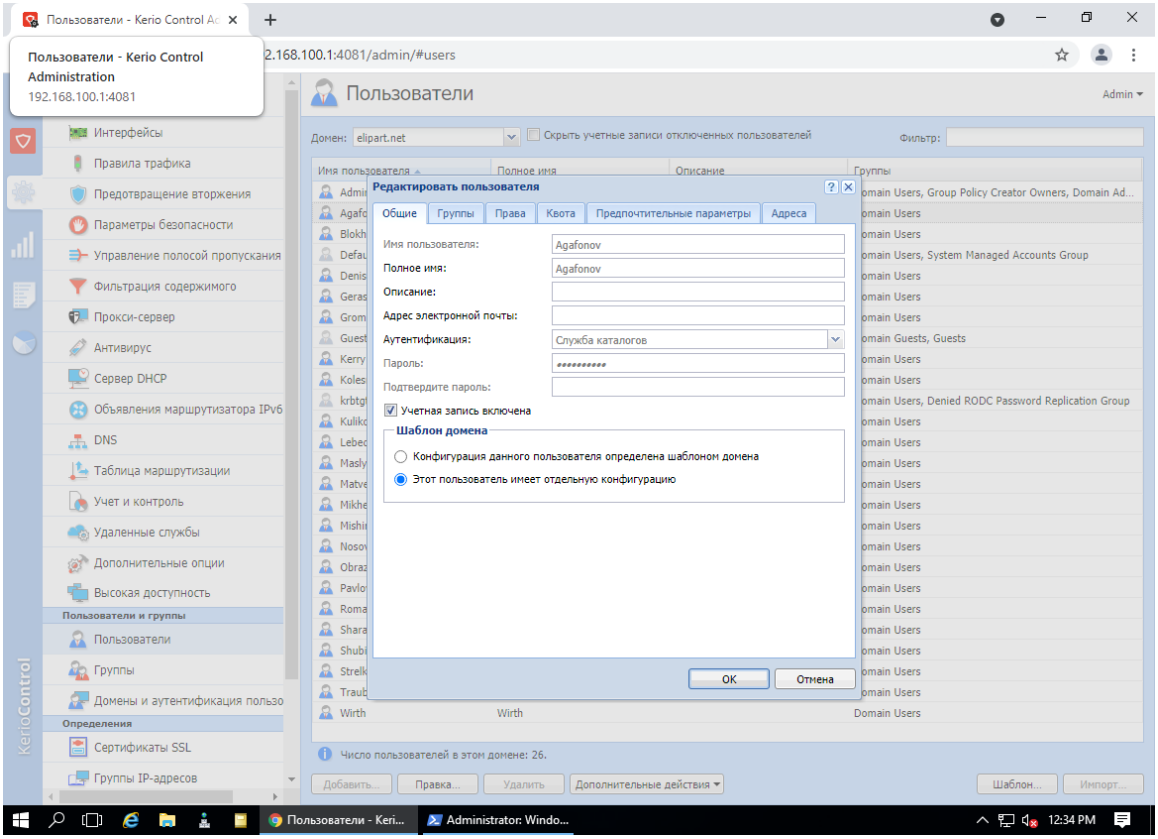

Домены и аутентификация пользователей - Kerio Control Administration
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Не является членом какого-либо домена.
Присоединить к домену...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы каталогов:
Microsoft® Active Directory®
Имя домена:
Дополнительно...
Применить
Восстановить
Присоединить к домену
Успешно. Брандмауэр сейчас является членом домена elipart.net.
Закрыть
Домены и аутентиф...
11:22 AM

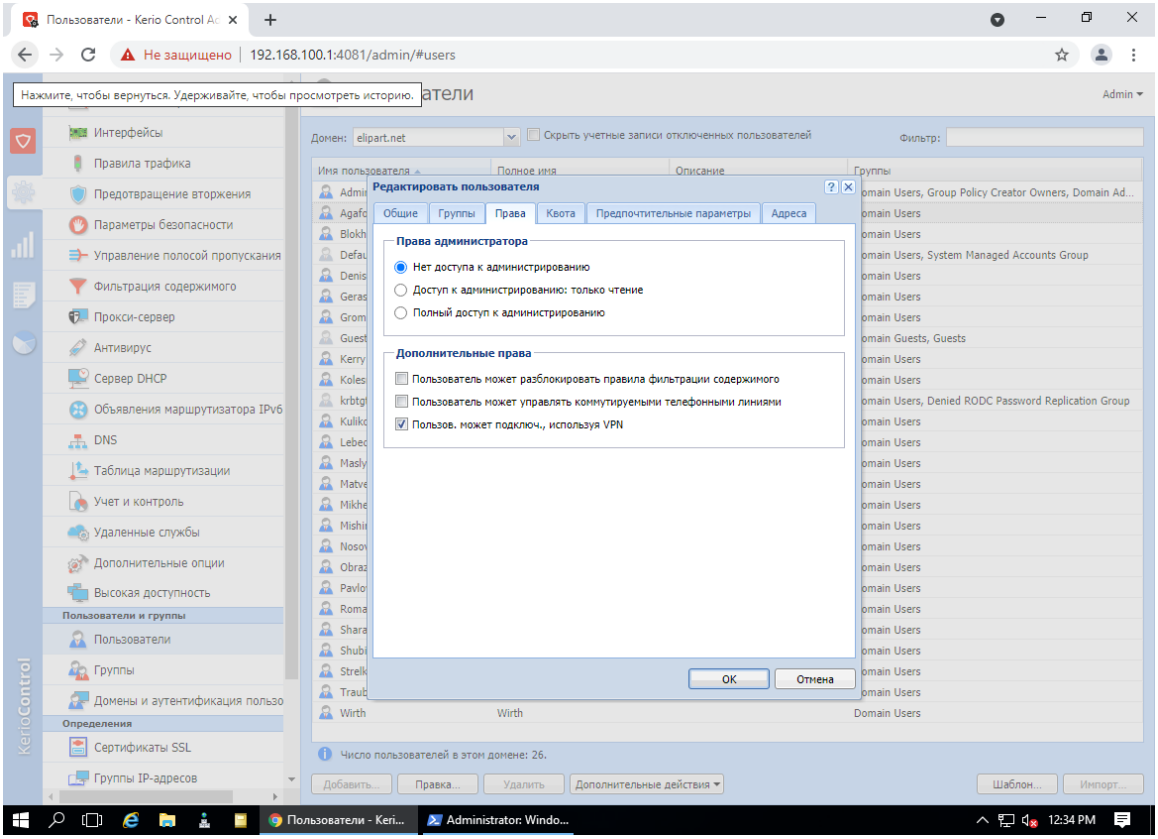

Домены и аутентификация пользователей - Kerio Control Administration
Не защищено | https://192.168.100.1:4081/admin/#domainsAndUserLogin
Домены и аутентификация пользователей
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Параметры аутентификации
Параметры безопасности
Службы каталогов
Гостевые интерфейсы
Член домена elipart.net.
Покинуть домен...
Сопоставить учетные записи пользователей и группы из службы каталогов
Домен
Тип службы каталогов:
Microsoft® Active Directory®
Имя домена:
elipart.net
Учетная запись с доступом для чтения в службе каталогов
Имя пользователя:
Administrator@elipart.net
Пароль:
Подключение
Автоматически подключаться к первому доступному серверу каталогов
Подключиться к указанным серверам каталогов:
Основной сервер:
Вспомогательный сервер:
Тест подключения
Дополнительно...
Применить
Восстановить
Домены и аутентиф...
11:22 AM


Пользователи - Kerio Control A
Не защищено | 192.168.100.1:4081/admin/#users
Пользователи
Admin
Панель мониторинга
Интерфейсы
Правила трафика
Предотвращение вторжения
Параметры безопасности
Управление полосой пропускания
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатора IPv6
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация пользо
Определения
Сертификаты SSL
Группы IP-адресов
KerioControl
Домен: elipart.net
Скрыть учетные записи отключенных пользователей
Фильтр:
Имя пользователя
Полное имя
Описание
Группы
Administrator Administrator Built-in account for administering... Domain Users, Group Policy Creator Owners, Domain Ad...
Agafonov Agafonov Domain Users
Blokhin Blokhin Domain Users
DefaultAccount DefaultAccount A user account managed by the ... Domain Users, System Managed Accounts Group
Denisov Denisov Domain Users
Gerasimov Gerasimov Domain Users
Gromov Gromov Domain Users
Guest Guest Built-in account for guest access ... Domain Guests, Guests
Kerry Kerry Domain Users
Kolesnikov Kolesnikov Domain Users
krbtgt krbtgt Key Distribution Center Service A... Domain Users, Denied RODC Password Replication Group
Kulikov Kulikov Domain Users
Lebedev Lebedev Domain Users
Maslyakov Maslyakov Domain Users
Matveev Matveev Domain Users
Mikheev Mikheev Domain Users
Mishin Mishin Domain Users
Nosov Nosov Domain Users
Obraztsova Obraztsova Domain Users
Pavlov Pavlov Domain Users
Romanov Romanov Domain Users
Sharapov Sharapov Domain Users
Shubin Shubin Domain Users
Strelkov Strelkov Domain Users
Trauberg Trauberg Domain Users
Wirth Wirth Domain Users
Число пользователей в этом домене: 26.
Добавить...
Правка...
Удалить
Дополнительные действия
Шаблон...
Импорт...
Пользователи - Keri...
Administrator: Windo...
12:31 PM

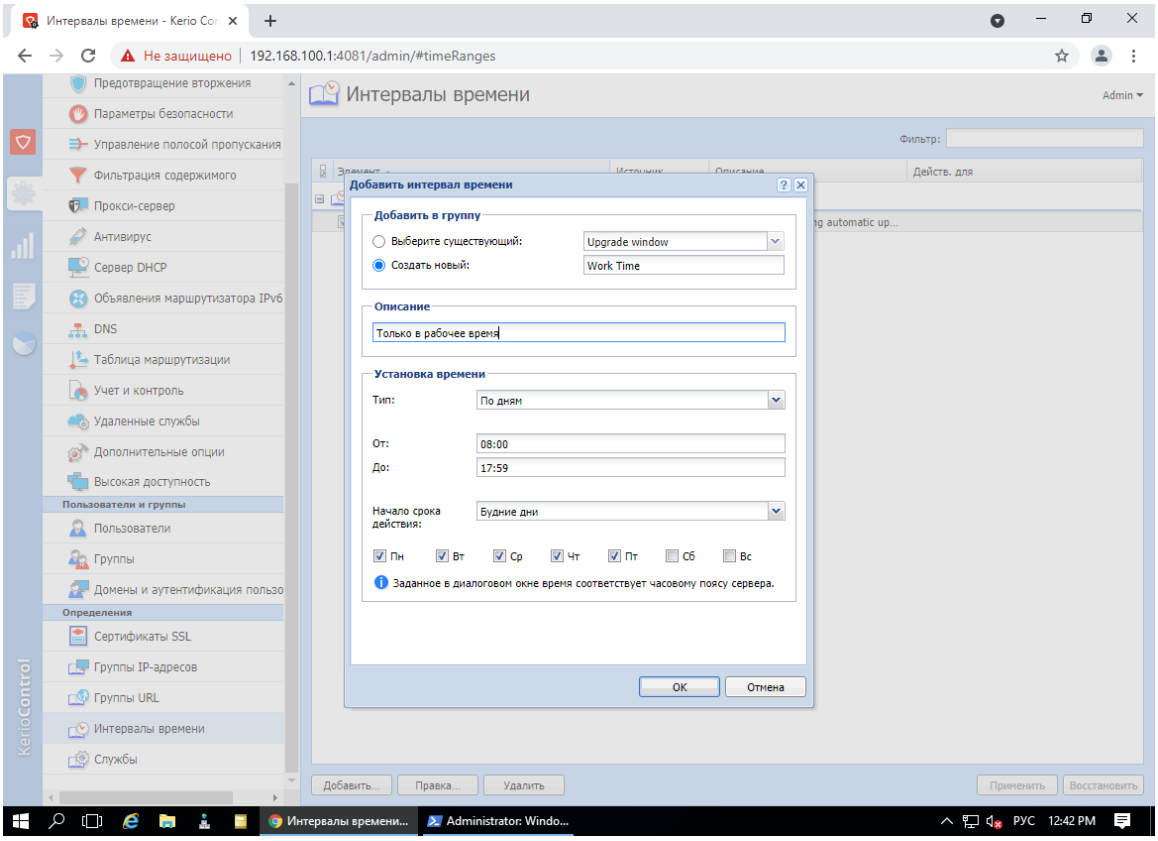
Шаг 7. Включите сервер VPN и произведите дополнительные настройки.

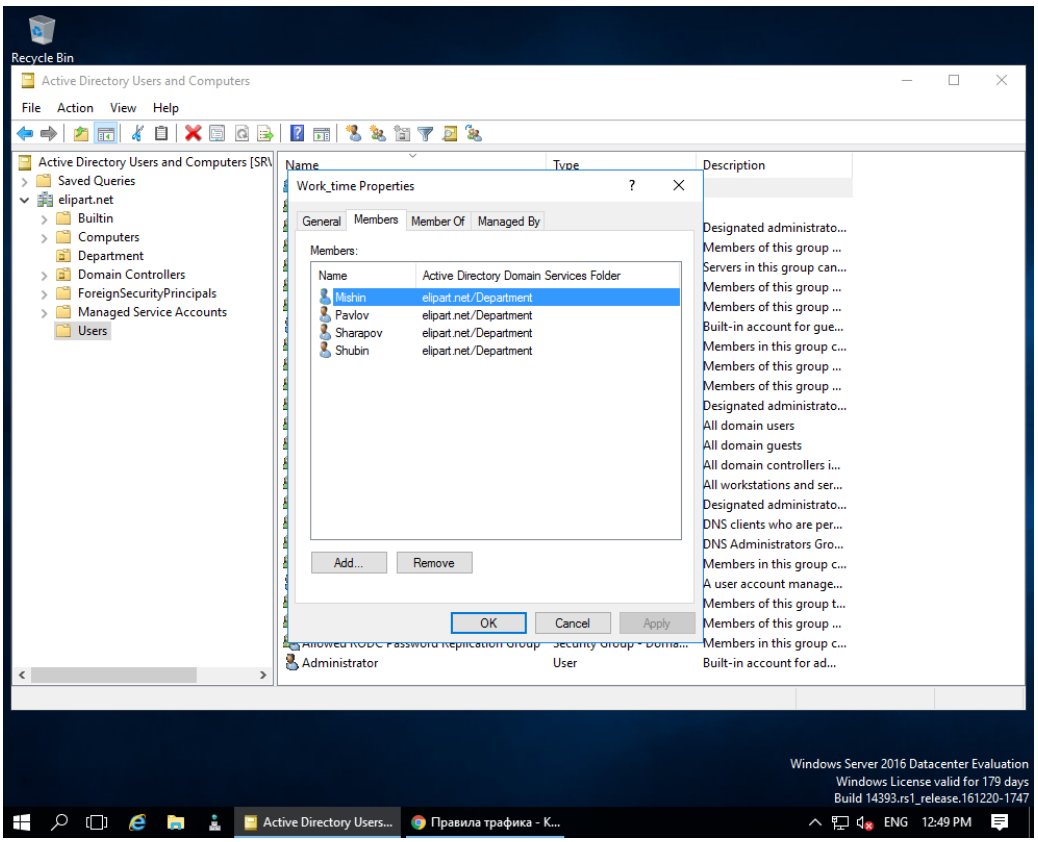


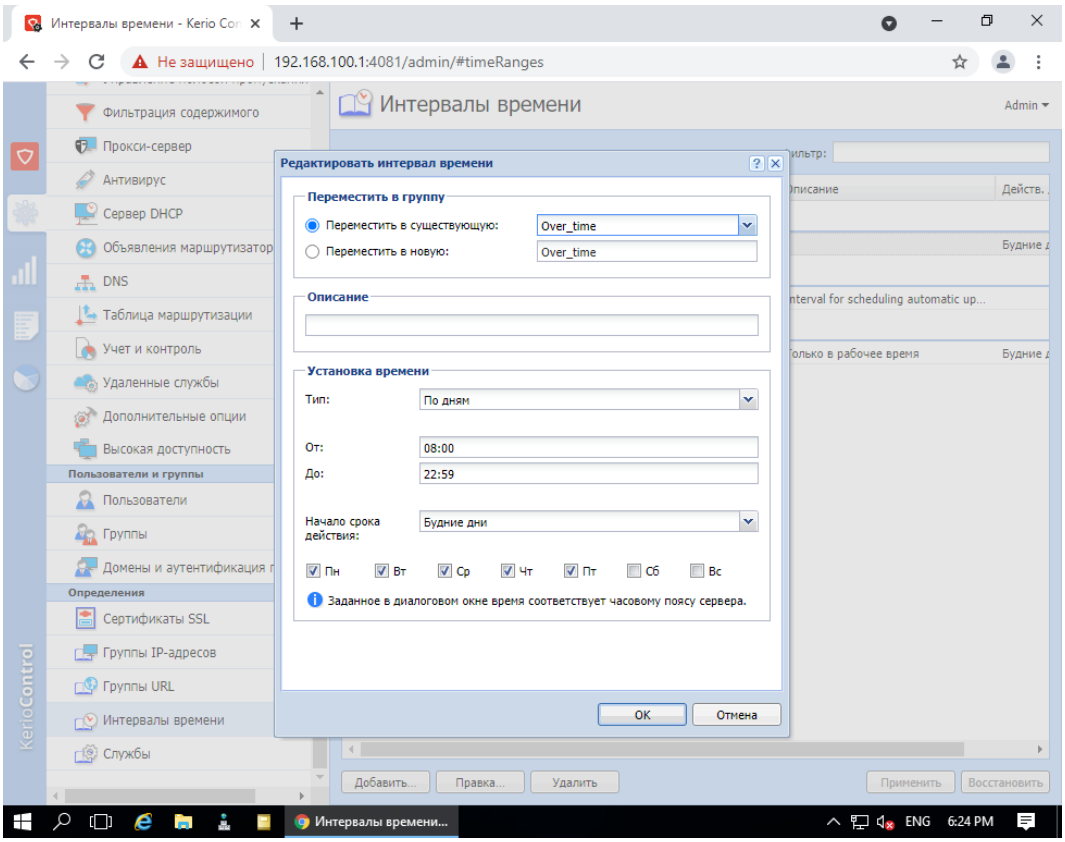


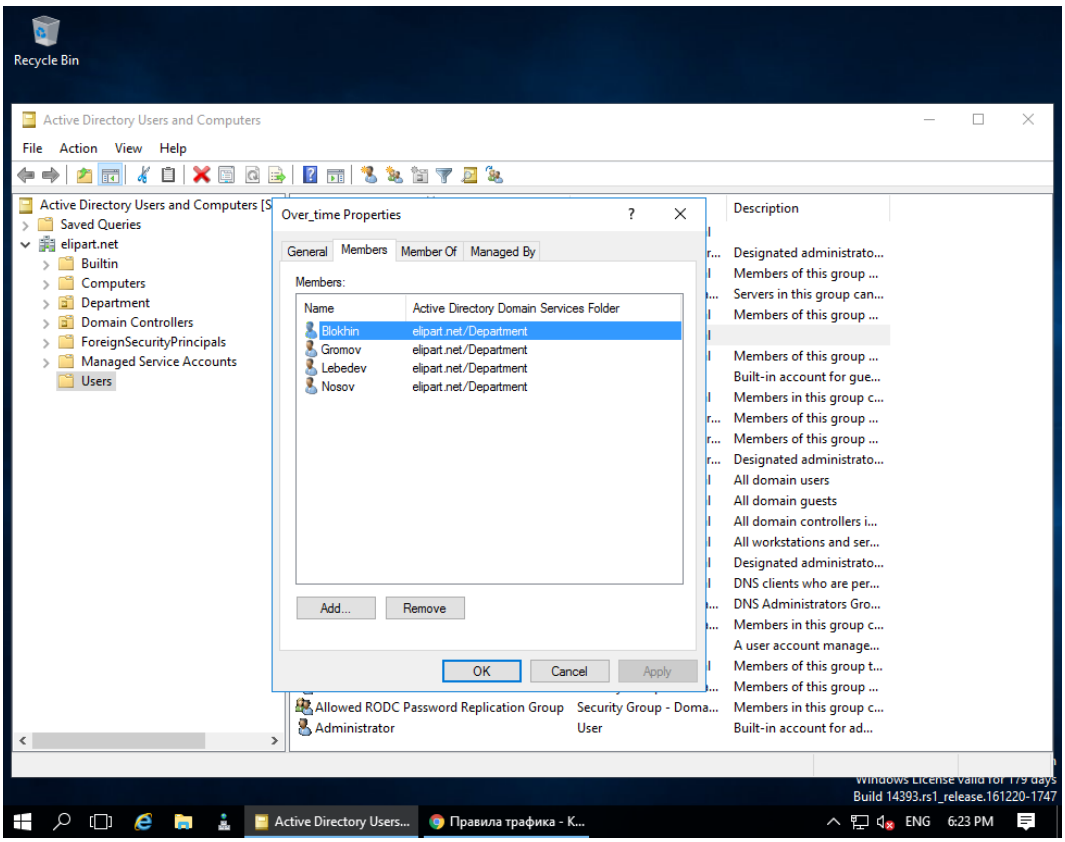


Шаг 8. Создайте правила для подключения к сети только в указанное время по VPN для дополнительной безопасности. Для руководящего состава необходимо создать исключения.

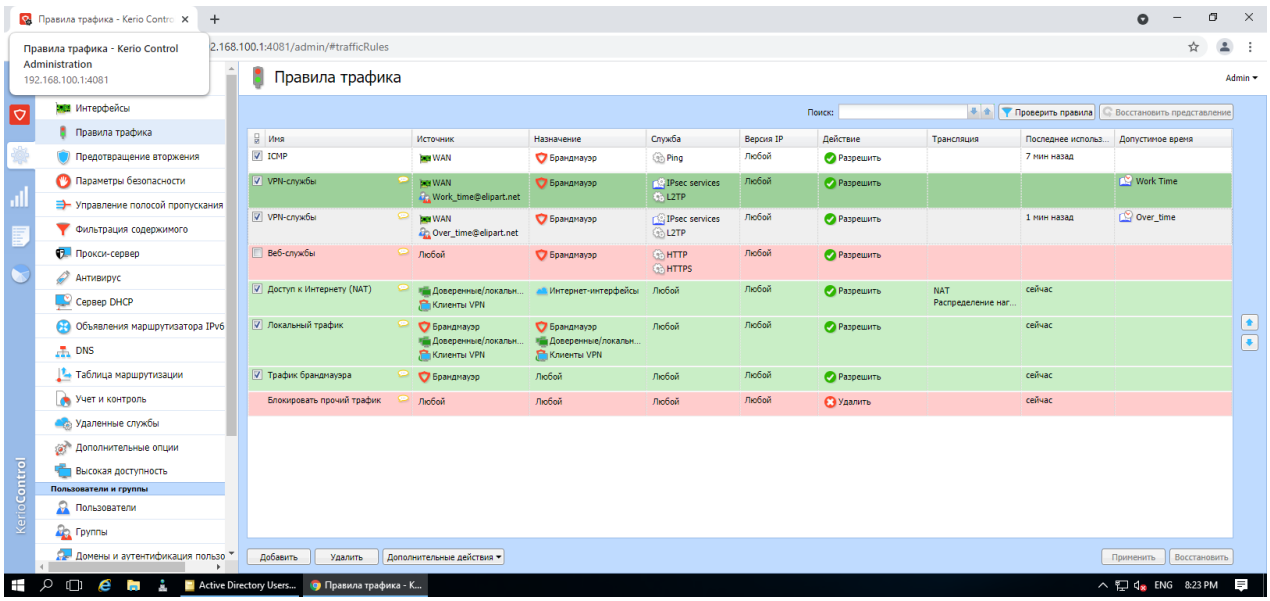


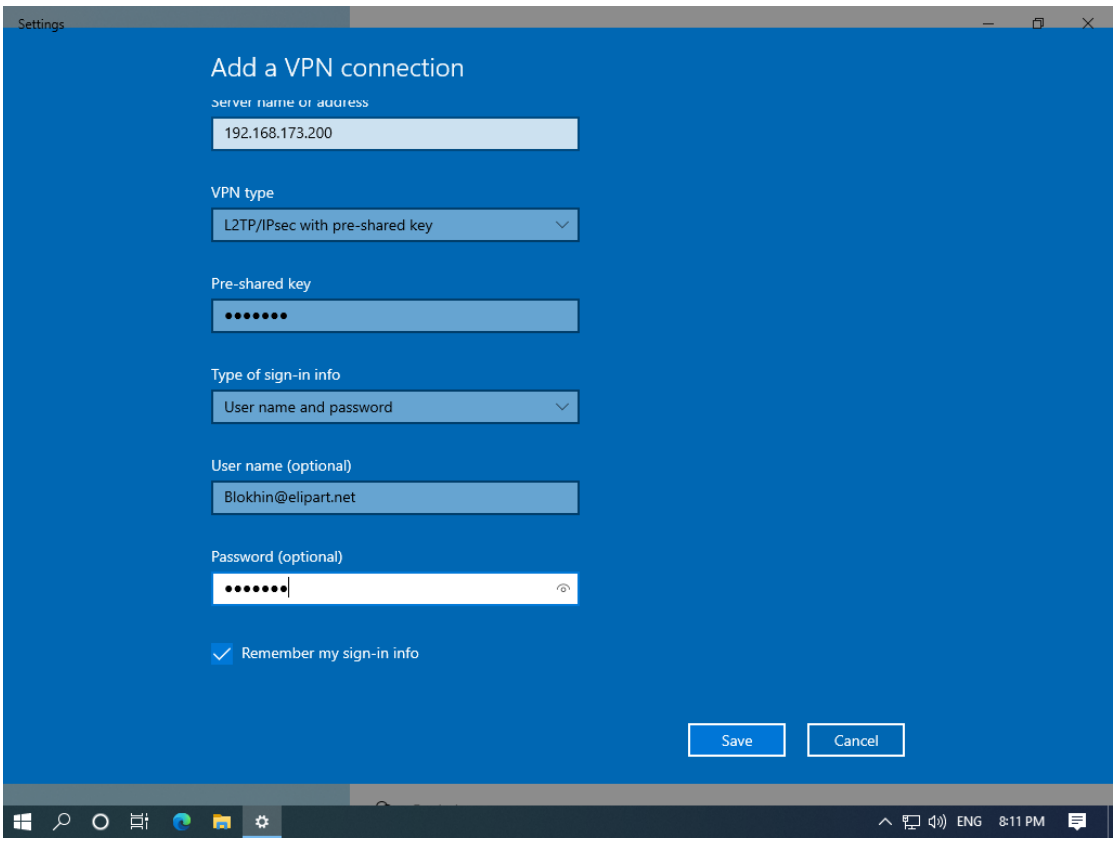

Recycle Bin
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [SRV
Saved Queries
elipart.net
Builtin
Computers
Department
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
Work_time Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
Mishin elipart.net/Department
Pavlov elipart.net/Department
Sharapov elipart.net/Department
Shubin elipart.net/Department
Add... Remove
OK Cancel Apply
Administrator User Built-in account for ad...
Windows Server 2016 Datacenter Evaluation
Windows License valid for 179 days
Build 14393.rs1_release.161220-1747
Active Directory Users...
Правила трафика - К...
ENG 12:49 PM

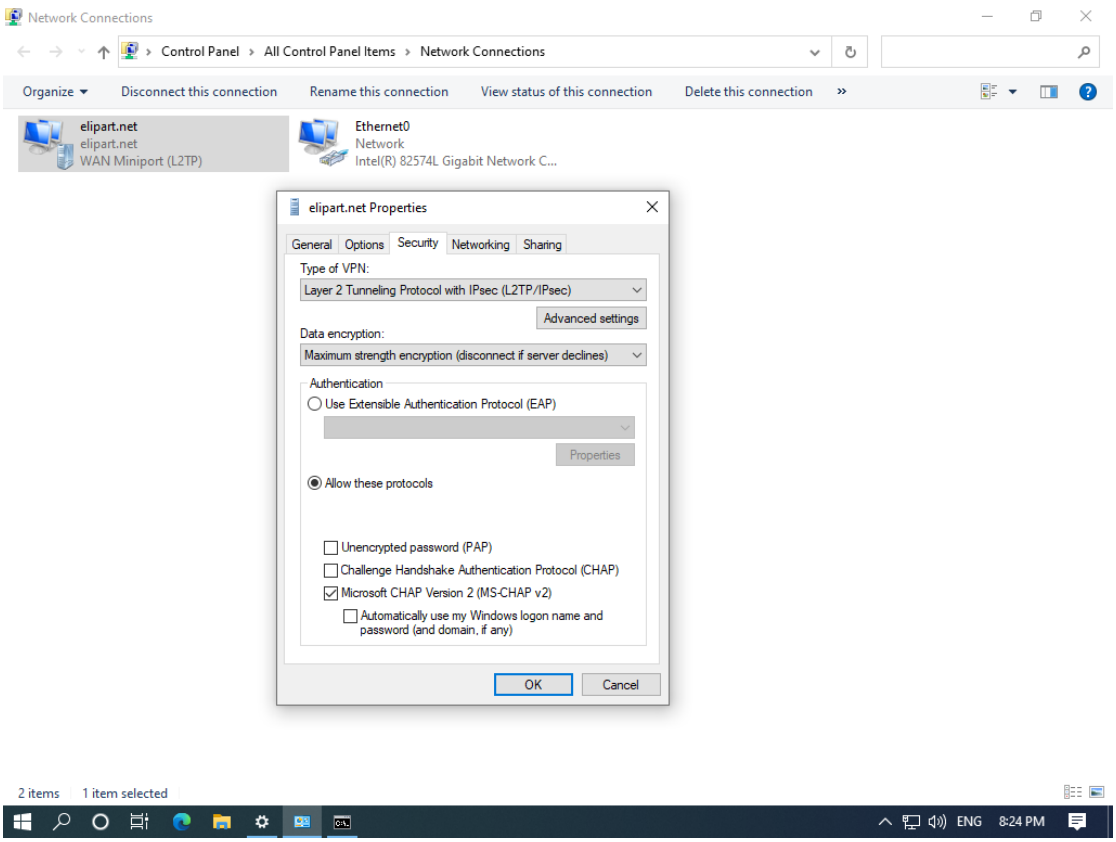

Интервалы времени - Kerio Con
Не защищено 192.168.100.1:4081/admin/#timeRanges
Интервалы времени
Admin
Фильтрация содержимого
Прокси-сервер
Антивирус
Сервер DHCP
Объявления маршрутизатор
DNS
Таблица маршрутизации
Учет и контроль
Удаленные службы
Дополнительные опции
Высокая доступность
Пользователи и группы
Пользователи
Группы
Домены и аутентификация
Определения
Сертификаты SSL
Группы IP-адресов
Группы URL
Интервалы времени
Службы
KerioControl
Редактировать интервал времени
Переместить в группу
Переместить в существующую: Over_time
Переместить в новую: Over_time
Описание
Установка времени
Тип: По дням
От: 08:00
До: 22:59
Начало срока действия: Будние дни
Пн Вт Ср Чт Пт Сб Вс
Заданное в диалоговом окне время соответствует часовому поясу сервера.
OK Отмена
Добавить... Правка... Удалить
Применить Восстановить
Интервалы времени...
ENG 6:24 PM

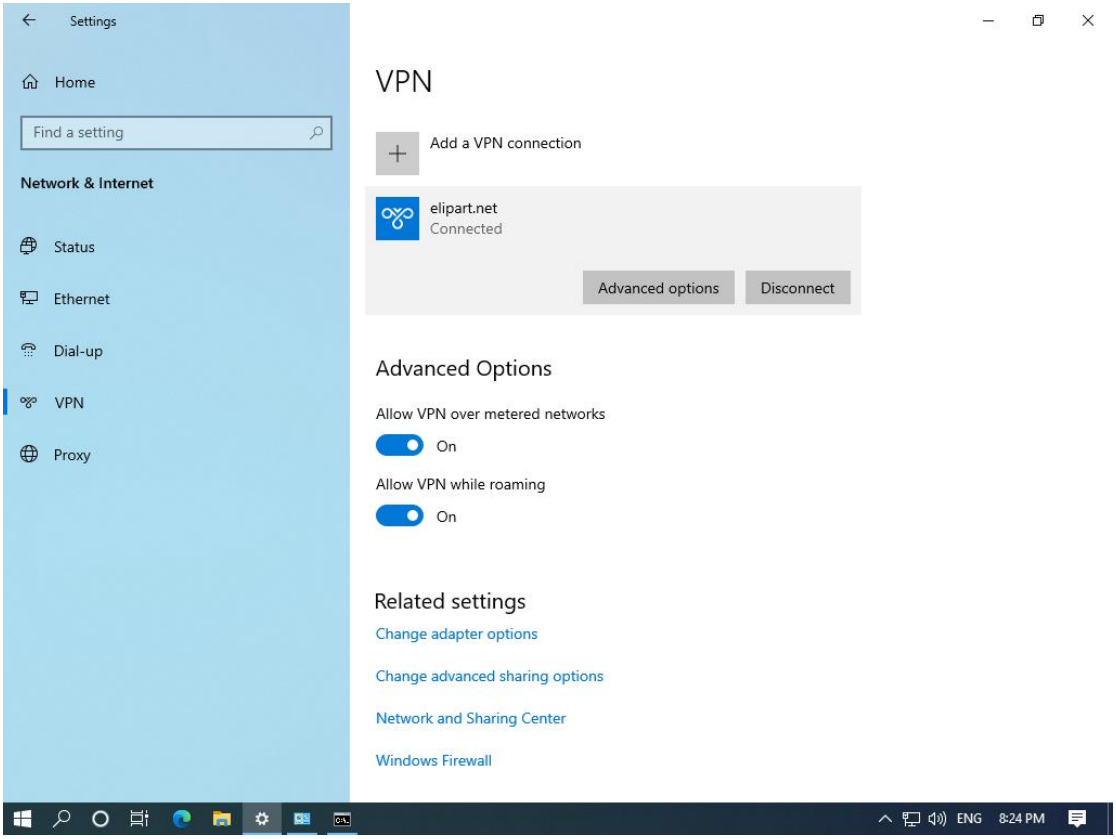


Шаг 9. Для осуществления подключения клиентов сети по VPN добавьте правила трафика.

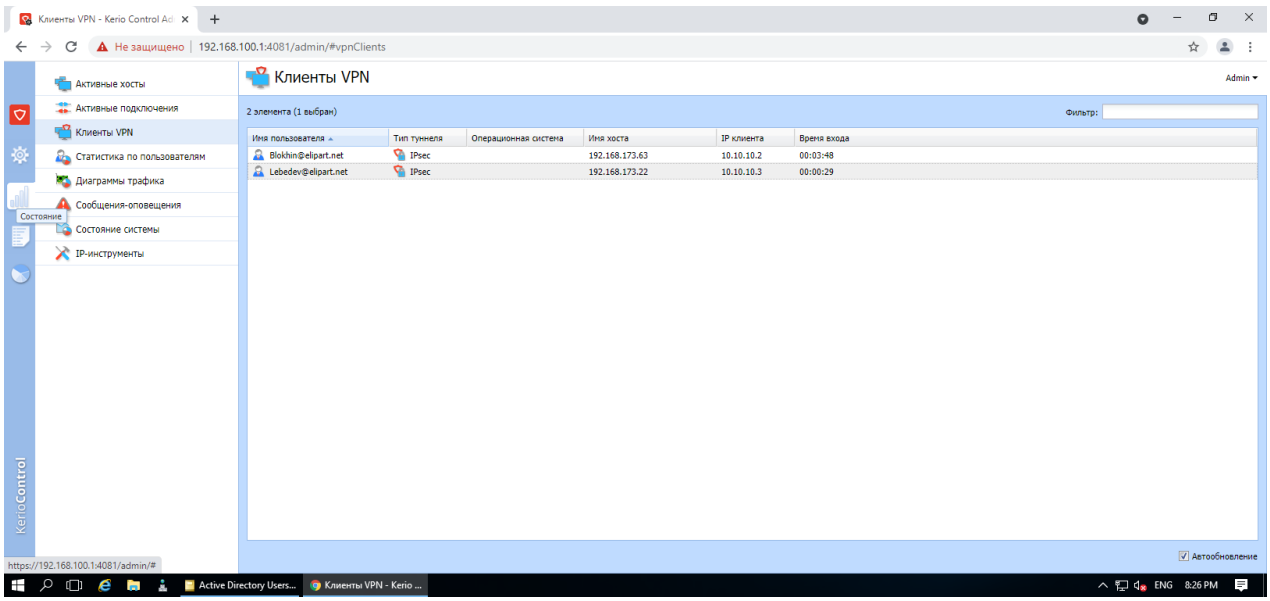


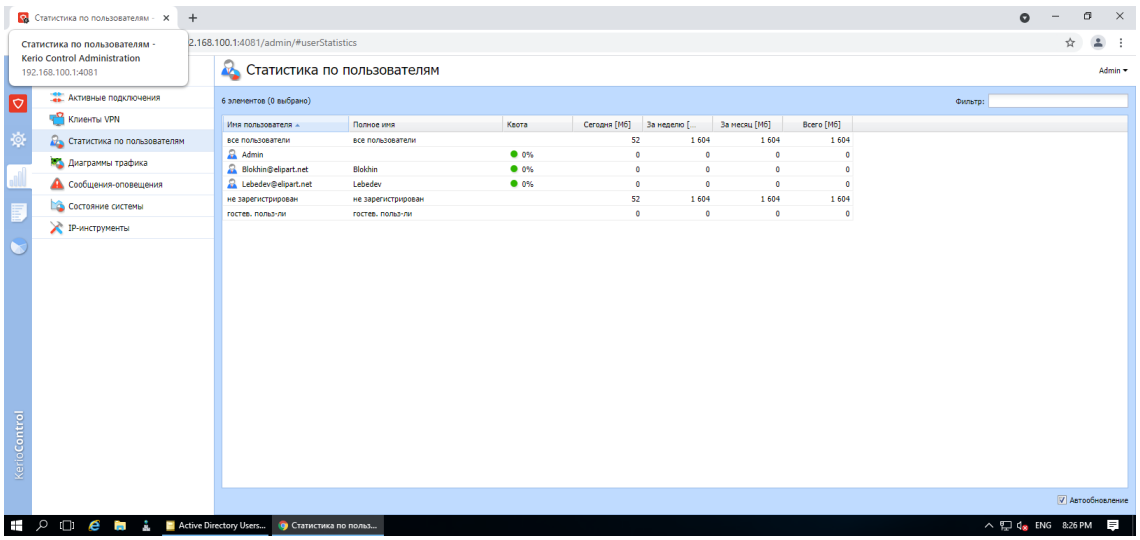

Settings
Add a VPN connection
192.168.173.200
VPN type
L2TP/IPsec with pre-shared key
Pre-shared key
Type of sign-in info
User name and password
User name (optional)
Blokhin@elipart.net
Password (optional)
Remember my sign-in info
Save
Cancel
ENG
8:11 PM

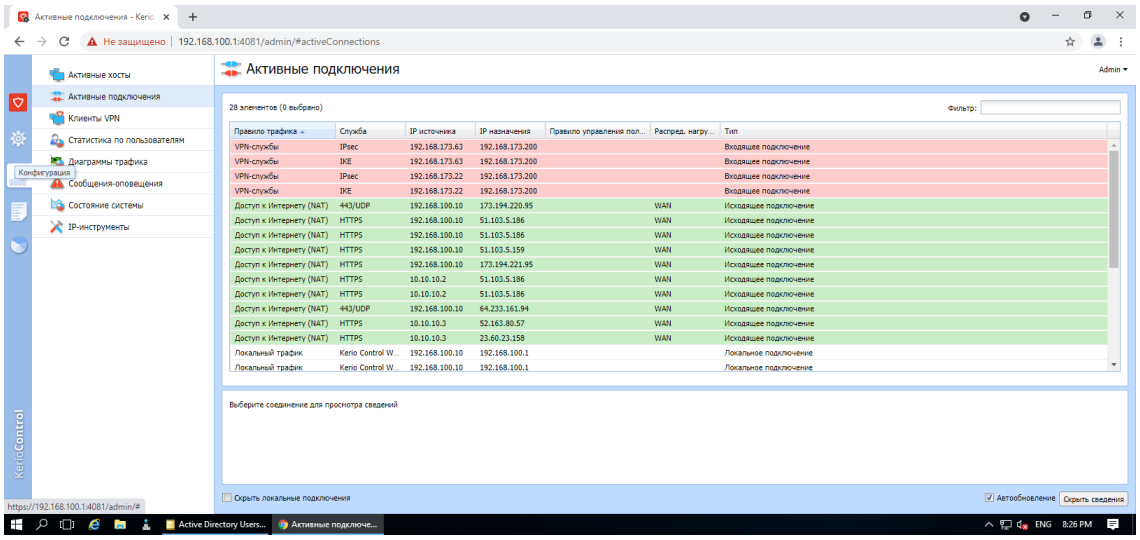

Network Connections
Control Panel › All Control Panel Items › Network Connections
Organize
Disconnect this connection
Rename this connection
View status of this connection
Delete this connection
elipart.net
elipart.net
WAN Miniport (L2TP)
Ethernet0
Network
Intel(R) 82574L Gigabit Network C...
elipart.net Properties
General
Options
Security
Networking
Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
Advanced settings
Data encryption:
Maximum strength encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK
Cancel
2 items
1 item selected
ENG
8:24 PM



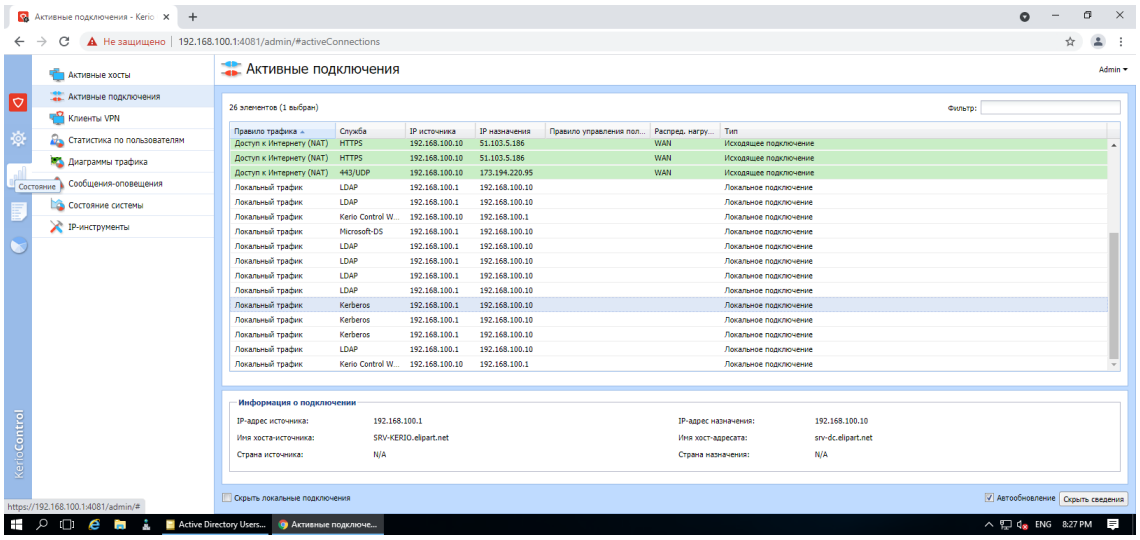
Шаг 10. Проверьте систему мониторинга для того, чтобы убедиться, что пользователи успешно подключились к VPN серверу.

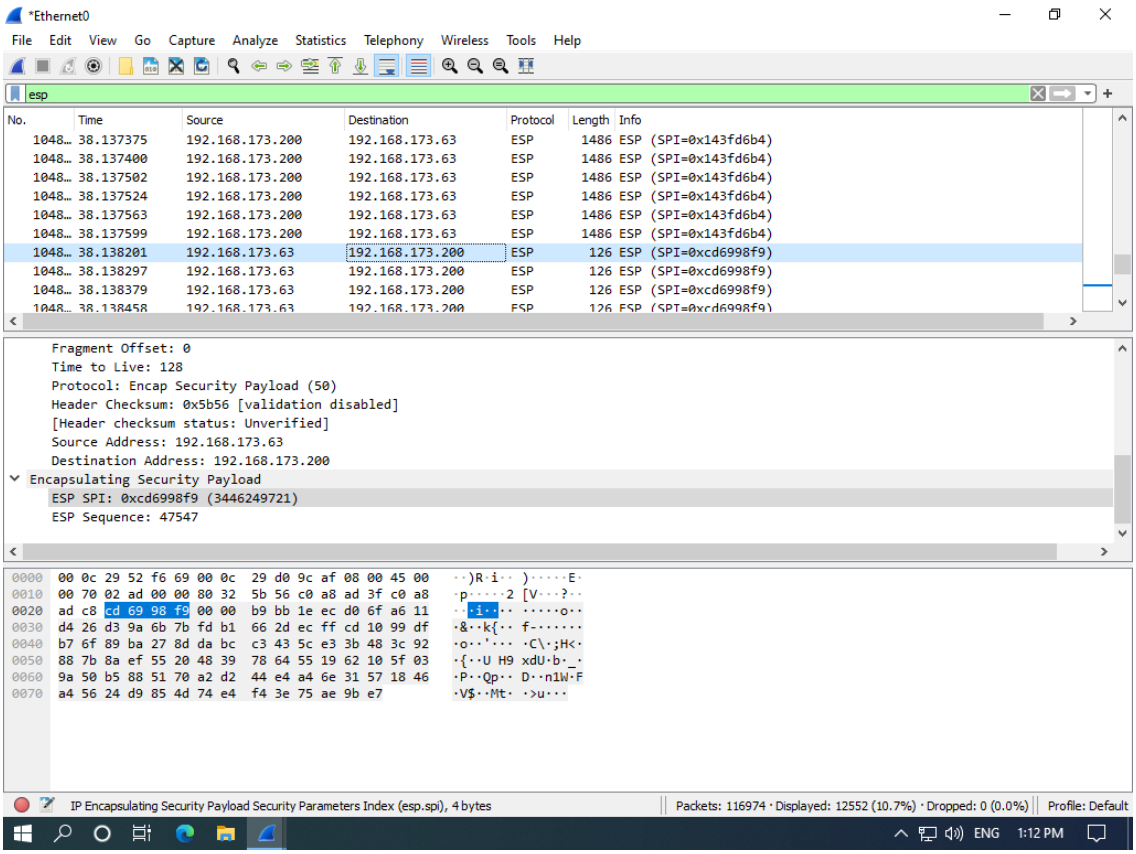


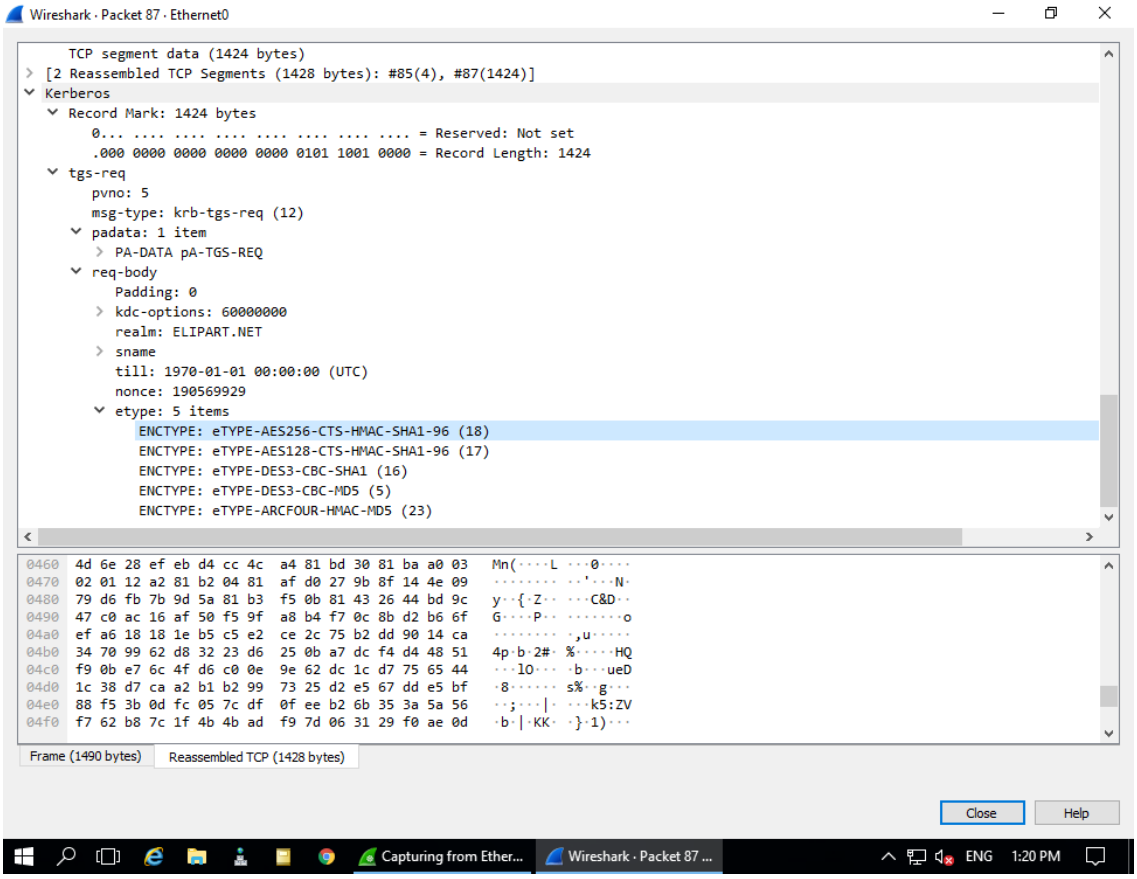




Шаг 11. Убедитесь, что вся информация о пользователях передается от Active Directory в зашифрованном виде.




*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
esp
No. Time Source Destination Protocol Length Info
1048… 38.137375 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.137400 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.137502 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.137524 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.137563 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.137599 192.168.173.200 192.168.173.63 ESP 1486 ESP (SPI=0x143fd6b4)
1048… 38.138201 192.168.173.63 192.168.173.200 ESP 126 ESP (SPI=0xcd6998f9)
1048… 38.138297 192.168.173.63 192.168.173.200 ESP 126 ESP (SPI=0xcd6998f9)
1048… 38.138379 192.168.173.63 192.168.173.200 ESP 126 ESP (SPI=0xcd6998f9)
Fragment Offset: 0
Time to Live: 128
Protocol: Encap Security Payload (50)
Header Checksum: 0x5b56 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.173.63
Destination Address: 192.168.173.200
Encapsulating Security Payload
ESP SPI: 0xcd6998f9 (3446249721)
ESP Sequence: 47547
0000 00 0c 29 52 f6 69 00 0c 29 d0 9c af 08 00 45 00
0010 00 70 02 ad 00 00 80 32 5b 56 c0 a8 ad 3f c0 a8
0020 ad c8 cd 69 98 f9 00 00 b9 bb 1e ec d0 6f a6 11
0030 d4 26 d3 9a 6b 7b fd b1 66 2d ec ff cd 10 99 df
0040 b7 6f 89 ba 27 8d da bc c3 43 5c e3 3b 48 3c 92
0050 88 7b 8a ef 55 20 48 39 78 64 55 19 62 10 5f 03
0060 9a 50 b5 88 51 70 a2 d2 44 e4 a4 6e 31 57 18 46
0070 a4 56 24 d9 85 4d 74 e4 f4 3e 75 ae 9b e7
IP Encapsulating Security Payload Security Parameters Index (esp.spi), 4 bytes
Packets: 116974 · Displayed: 12552 (10.7%) · Dropped: 0 (0.0%)
Profile: Default
ENG 1:12 PM


Wireshark · Packet 87 · Ethernet0
TCP segment data (1424 bytes)
[2 Reassembled TCP Segments (1428 bytes): #85(4), #87(1424)]
Kerberos
Record Mark: 1424 bytes
0... .... = Reserved: Not set
.000 0000 0000 0000 0000 0101 1001 0000 = Record Length: 1424
tgs-req
pvno: 5
msg-type: krb-tgs-req (12)
padata: 1 item
PA-DATA pA-TGS-REQ
req-body
Padding: 0
kdc-options: 60000000
realm: ELIPART.NET
sname
till: 1970-01-01 00:00:00 (UTC)
nonce: 190569929
etype: 5 items
ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
ENCTYPE: eTYPE-DES3-CBC-SHA1 (16)
ENCTYPE: eTYPE-DES3-CBC-MD5 (5)
ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
0460 4d 6e 28 ef eb d4 cc 4c a4 81 bd 30 81 ba a0 03
0470 02 01 12 a2 81 b2 04 81 af d0 27 9b 8f 14 4e 09
0480 79 d6 fb 7b 9d 5a 81 b3 f5 0b 81 43 26 44 bd 9c
0490 47 c0 ac 16 af 50 f5 9f a8 b4 f7 0c 8b d2 b6 6f
04a0 ef a6 18 18 1e b5 c5 e2 ce 2c 75 b2 dd 90 14 ca
04b0 34 70 99 62 d8 32 23 d6 25 0b a7 dc f4 d4 48 51
04c0 f9 0b e7 6c 4f d6 c0 0e 9e 62 dc 1c d7 75 65 44
04d0 1c 38 d7 ca a2 b1 b2 99 73 25 d2 e5 67 dd e5 bf
04e0 88 f5 3b 0d fc 05 7c df 0f ee b2 6b 35 3a 5a 56
04f0 f7 62 b8 7c 1f 4b 4b ad f9 7d 06 31 29 f0 ae 0d
Frame (1490 bytes)
Reassembled TCP (1428 bytes)
Close
Help
Capturing from Ether...
Wireshark · Packet 87 ...
ENG 1:20 PM

После завершения настройки проанализируем трафик из вне сети и внутри, где мы можем убедиться, что обмен данными происходит в зашифрованном виде.

Вывод. Выполнив все шаги, мы установили и полностью настроили шлюз Kerio Control для работы. Также был включен сервер VPN и разрешен доступ для пользователей. В результате осуществлено подключение по VPN и проверена работоспособность сети.

4 Экономическое обоснования выбора решения

При построении корпоративной сети нужно учитывать ежегодную прибыль и потери при простоях в случае карантина.

Произведен расчет экономической эффективности построения корпоративной сети на базе VPN технологии.

Таблица 4.1 – Показатель прибыли за год.

	Прибыль, тг
Январь	11 843 516
Февраль	10 564 824
Март	13 487 554
Апрель	12 499 543
Май	13 694 487
Июнь	11 849 661
Июль	9 016 495
Август	10 598 462
Сентябрь	16 449 533
Октябрь	10 649 554
Ноябрь	11 356 642
Декабрь	13 664 995
Итого за 12 месяцев	**145 675 266**

Вычислена средняя прибыль за месяц:

$$П_{сред/месяц} = \frac{\sum П}{12} = \frac{145675266}{12} = 12\ 139\ 606$$

$$П_{рабочий/день} = \frac{П_{сред/месяц}}{21} = \frac{12139606}{21} = 578\ 076$$

Таблица 4.2 – Сравнительная таблица

Вендор	**Kerio Control Server**	**Fortinet**	**PaloAlto**	**Cisco**	**Check Point**
Стоимость, тг	777 256	1 362 519	1 542 960	4 015 982	6 210 414

Таблица 4.3 – Капитальные затраты

№ п/п	**Наименование**	**Кол-во**	**Стоимость**
1	Сервер	1	3 857 400
2	Серверный шкаф (в комплекте)	1	230 000
3	Источник бесперебойного питания	1	152 600
4	Windows Server 2016	1	416 502
5	Kerio Control Server	1	777 256
		Итого	5 433 758

Суммарное потребление электроэнергии в месяц, применяем формулу

$$W = P*(t_д * t_{чп} * t_н)*T$$

где:

P - расход электроэнергии (кВт, мощность),

$t_д$ - время работы оборудования по дневной ставке,

$t_{чп}$- время работы оборудования в часы пик,

$t_н$ - время работы оборудования в ночное время,

T - количество суток электроприемника,

$W_{январь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{февраль}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 28 = 13 278
$W_{март}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{апрель}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 30 = 14227
$W_{май}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{июнь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 30 = 14 227
$W_{июль}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{август}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{сентябрь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 30 = 14 227
$W_{октябрь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701
$W_{ноябрь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 30 = 14 227
$W_{декабрь}$ = 2 * (12 * 10,6 + 4 * 21,7 + 8 * 2,89) * 31 = 14 701

Таблица 4.4 – Тарифы на электроэнергию.

	Дневная ставка тарифа (с 07.00 до 19.00) за 1 кВт-ч	Ставка тарифа в часы максимума (с 19.00 до 23.00) за 1 кВт-ч	Ночная ставка тарифа (с 23.00 до 07.00) за 1 кВт-ч
Стоимость, тг	10,16	21,07	2,89

Суммарное потребление электроэнергии за 12 месяцев:

$$W \sum = 173\ 098 \text{ тг.}$$

Таблица 4.5 – Операционные затраты.

№ п/п	Наименование	12 месяцев
1	Фонд оплаты труда системного администратора	3 313 656
2	Затраты на электроэнергию	173 098
	Итого в год	3 486 754

Расчет окупаемости проекта:

$$E = \frac{C_{кап} + C_{оп}}{П_{рабочий/день}}$$

где:

$C_{кап}$- капитальные затраты,

$C_{оп}$ – операционные затраты,

$П_{10\%\ рабочий/день}$ – прибыль за один рабочий день.

$$E = \frac{5433758 + 3486754}{5780{,}7} = 154{,}3 \text{ рабочих дня} \approx 7{,}7 \text{ месяцев.}$$

В случае карантина срок окупаемости проекта составит 154 рабочих дня или 7,7 месяцев с учетом инвестиций 10% от суммы ежедневного дохода за один рабочий день.

5 Безопасность жизнедеятельности

5.1 Серверное помещение

Серверная — это телекоммуникационная комната, в которой находится распределительное устройство и большое количество активного телекоммуникационного оборудования. В серверной комнате можно разместить точки распределения и пассивные распределительные устройства (патч-панели, крестовины, распределительные коробки). В стандартах нет критерия для определения типа (серверная или кроссоверная) телекоммуникационной комнаты по количеству установленного активного оборудования. Поэтому тип телекоммуникационного помещения определяет установщик информационной системы или заказчик [25].

Ниже приводятся часть требований и рекомендаций к серверному помещению, которые разработаны на основе стандарта TIA/EIA-569:

Размещение серверного помещения. Серверную следует размещать как можно ближе к основным кабельным каналам. Серверную комнату желательно разместить рядом с основной точкой распространения (Main Cross, MC), а по возможности установить основную точку распространения в серверной. Не размещайте серверную рядом с лифтовыми шахтами, лестничными клетками, вентиляционными камерами или другими элементами здания, которые могут ограничить расширение аппаратного помещения в будущем.

Рекомендуемые размеры серверного помещения. Размер серверного помещения выбирается исходя из размера обслуживаемой рабочей области и количества устанавливаемого оборудования. Важно учесть не только размеры самого оборудования, но и способы монтажа, обеспечения доступа и обслуживания оборудования, возможность установки дополнительных устройств. Высота серверного помещения должна быть не менее 2,44 метра. Минимально рекомендуемый размер серверной комнаты должен быть не менее 14 м^2. Рекомендуется выделить под серверное помещение 0,09 м^2 площади на каждые 10 м^2 обслуживаемой рабочей площади.

Защита от протечек воды. Избегайте размещения серверной комнаты ниже уровня земли, если она не защищена от проникновения воды. Трубопроводы и дренажные системы нельзя размещать в серверном помещении, если они не предназначены для работы оборудования и специальных систем, расположенных в серверном помещении. Если есть вероятность протечки воды в серверную, рекомендуется установить слив. Например, можно сделать в полу сливное отверстие. Если в серверной устанавливаются спринклеры, рекомендуется установить дренажные каналы под трубы, подходящие к осколкам, чтобы защитить оборудование от возможных протечек.

Окна, дверь и дверной проем. В качестве серверной рекомендуется использовать комнату без окон. Если в серверной есть окна, то окна необходимо заделать кирпичом. Дверной проем должен быть шириной не менее 0,91 м и высотой не менее 2 м. Дверь должна быть заперта, чтобы ограничить доступ в кроссоверную. Допускается использование раздвижной двери. Распашная дверь должна открываться наружу, проем двери должен быть не менее 1800. Если вы планируете вывозить все оборудование в серверной, рекомендуется установить двустворчатую дверь с минимальной шириной проема не менее 1,82 м и высотой не менее 2,28 м.

Отделка стен, потолка и пола. Стены, потолок и пол должны иметь покрытие, препятствующее выходу, оседанию и накоплению пыли на поверхности. Потолок обязательно должен иметь гидроизоляцию, чтобы предотвратить протекание воды. Стены следует покрасить светлой краской.

Микроклимат (температура, влажность, вентиляция). Система контроля и управления микроклиматом должна обеспечивать заданный уровень влажности и температуры в серверной комнате, необходимый для нормальной работы активного оборудования. Система микроклимата должна обеспечивать поддержание температурного режима не только летом, но и зимой и рассчитана на круглосуточную непрерывную работу. Если централизованная система микроклимата в здании не может обеспечить непрерывную работу и заданный уровень температуры и влажности, то в серверной необходимо установить автономную систему. Требуется следить за тем, чтобы давление воздуха в серверной было больше, чем в соседних помещениях. Рекомендуется менять воздух в серверной не реже одного раза в час, если в помещении постоянно работает обслуживающий персонал.

Рекомендуется использовать систему очистки и фильтрации поступающего воздуха в аппаратном помещении. Если в здании установлена система резервного электроснабжения, система поддержки микроклимата в серверном помещении должна быть подключена к системе резервного электроснабжения.

Вибрация и электромагнитные помехи. Вибрация отрицательно сказывается на работе активного оборудования, контактов и соединений. В диапазоне частот до 25 Гц амплитуда колебаний не должна превышать 0,1 мм. Серверная должна располагаться вдали от источников электромагнитных помех на таком расстоянии, чтобы напряженность электрического поля в серверной не превышала 3 В/м во всем частотном спектре.

Электропитание и электрические розетки. Рекомендуется установить не менее двух отдельных блоков двойных розеток. Блоки розеток рекомендуется питать от разных кабелей питания, розетки должны быть рассчитаны на переменный ток до 16А. Дополнительно требуется установка агрегатов с двойными розетками через каждые 1,8 м вдоль стены на высоте не менее 0,15 м от уровня пола. Электропитание в серверной должно осуществляться через специальный кабель питания, желательно непосредственно от главного распределительного щита. Если установлена система резервного электропитания, серверная комната должна питаться от системы резервного электропитания. Для серверной необходимо установить отдельный электрощиток. В серверной допускается установка источников бесперебойного питания (ИБП) до 100 кВА. ИБП мощностью более 100 кВА необходимо устанавливать в отдельном помещении.

Заземление. Основная телекоммуникационная заземляющая шина должна быть установлена в аппаратном помещении, к которому должны быть подключены заземляющие и соединительные провода от монтажных конструкций, телекоммуникационного оборудования и металлических трубопроводов.

Средства распределения кабелей и организации кабельных потоков. Для разводки кабелей и организации кабельных потоков в телекоммуникационной комнате необходимо использовать кабельные каналы и органайзеры. Средства распределения и организации кабельных потоков должны быть надежно закреплены, выдерживать вес кабеля и обеспечивать защиту и разводку кабелей с минимально допустимым радиусом изгиба кабеля. Кабельные каналы должны быть проложены от кабельного ввода в телекоммуникационную комнату до телекоммуникационных шкафов. Кабельные каналы, расположенные под потолком, должны быть открытыми и доступными для дальнейших работ по прокладке кабелей, шнуров или перемычек.

Правила противопожарной безопасности для серверного помещения. После прокладки кабелей необходимо заделать все кабельные вводы в серверной огнестойким материалом, для этого можно использовать специальные заглушки, установленные в кабельный ввод, которые в случае пожара расширяются, заблокировать пространство и предотвратить распространение огня и дыма. Потолки, стены и перегородки серверного

помещения должны быть пожаробезопасными и обеспечивать огнестойкость не менее 45 минут. Дверь должна обеспечивать огнестойкость не менее 36 минут. Дверь может быть изготовлена из трудно сгораемого материала толщиной не менее 40 мм без внутренних пустот, а можно использовать деревянную дверь, но покрыть ее слоем асбеста или покрыть листовой сталью толщиной минимум 4 мм с обеих сторон. В серверной без окон следует устанавливать вытяжные шахты с ручным или автоматическим открыванием для удаления дыма в случае пожара. Площадь шахт должна составлять не менее 0,2% от площади помещения, а расстояние от любой точки помещения до шахты не должно быть более 20 метров. Если брызговики устанавливаются в серверной, рекомендуется закрывать их крышки защитными сетчатыми колпачками, чтобы избежать случайного срабатывания планок. Опоры и стойки фальшполов должны быть из огнестойкого материала. Плиты фальшпола должны быть изготовлены из негорючего материала или материала с пределом огнестойкости 30 минут. Верхнее покрытие плит фальшпола может быть выполнено из горючего материала.

Оборудование системами серверного помещения. Серверное помещение должна быть оборудована системами:

- охранной сигнализации;
- пожарной сигнализации;
- пожаротушения;
- кондиционирования и вентиляции;
- освещения и аварийного освещения.

5.2 Охрана труда при работе с вычислительной техникой

Вычислительная техника (ВТ) все чаще проникает во все сферы нашей жизни. Количество специалистов, работающих с персональным компьютером (ПК), который становится их основным рабочим инструментом, постоянно растет. Ни экономические, ни научные достижения сейчас невозможны без быстрой и четкой передачи информации и без специально обученного персонала. Беспрецедентная скорость получения визуальной информации и ее передачи адресату, а значит, и возможность максимально эффективного практического использования этой информации — вот основные причины всеобщей компьютеризации [26].

Вредные факторы при работе с ВТ:

- излучения;
- возможность попадания под действие тока;
- астенопия;
- психофизиологическая напряженность труда.

Излучения. Рабочий ПК генерирует следующие типы излучения: рентгеновское, ультрафиолетовое, электромагнитное, инфракрасное и электростатическое. Доля рентгеновского излучения невелика. Изображение на экране появляется в результате свечения монитора на внутренней поверхности

экрана под действием электронного пучка. Когда электроны сталкиваются с поверхностью, они генерируют тормозное излучение, в том числе рентгеновское. Источником ультрафиолетового излучения является плазменный разряд на внутренней поверхности экрана. Источником инфракрасного излучения является блок питания, а также электронно-лучевая трубка. Компьютер - источник электромагнитного излучения.

Основную опасность для здоровья пользователя представляет собой электромагнитное излучение в диапазоне 20 Гц - 400 кГц, создаваемое отклоняющей системой кинескопа и видеомонитором. Существует множество экспериментальных данных, свидетельствующих о влиянии электромагнитных полей на живой организм (на молекулярном и клеточном уровне) – нервную, эндокринную, иммунную и кроветворную системы организма.

Установлено, что наиболее опасна низкочастотная составляющая электромагнитного поля (до 100 Гц), которая способствует изменению биохимической реакции в крови на клеточном уровне. Это приводит к появлению у человека симптомов раздражительности, нервного напряжения и стресса, вызывает осложнения при беременности и в несколько раз увеличивает вероятность выкидышей, способствует нарушению репродуктивной функции и возникновению онкологических заболеваний.

Видеомонитор компьютера создает вокруг себя электромагнитное поле как низкой, так и высокой частоты, которое способствует появлению электростатического поля и приводит к деионизации воздуха вокруг монитора, что, в свою очередь, влияет на развитие клеток тканей организма, увеличивается вероятность катаракты.

Под действием электромагнитного поля присутствующие в воздухе заряженные частицы пыли разгоняются и разлетаются, оседая на предметах вокруг компьютера, падая на лицо, руки оператора. Это вызывает ощущение стягивания кожи, а у чувствительных людей - аллергия, конъюнктивит, блефарит (воспалительные заболевания слизистых оболочек глаз, век).

Астенопия (быстрая утомляемость глаз). При длительной работе за компьютером (более 4 часов в сутки) наблюдается нарушение аппомодации и цветового восприятия. Астенопию вызывают:

- мерцание экрана;
- плохая освещенность как рабочего места, так и экрана, высокая резкость, наличие бликов и отражений, неоптимальное соотношение яркости и контрастности.

Все это влияет не только на глаза, но и на мозг, который анализирует изображение и дает команду рукам.

Психофизиологическая напряженность труда проявляется в перенапряжении анализаторов, длительном пребывании в вынужденном положении.

Из-за чрезмерного психофизиологического напряжения, выраженное в анализе полученной информации, в постоянно повторяющихся движениях рук, в статических нагрузках на опорно-двигательном аппарате, общее

недомогании, головных болях, скелетно-мышечная боль развивается. Особенно много жалоб на боли при работе с клавиатурой – в результате монотонных однообразных движений развивается синдром длительных статических нагрузок (СДСН), СДСН проявляется в виде танденитов – воспалительных процессов в тканях сухожилий. Чаще всего встречается синдром запястного канала. При непрерывно повторяющихся движениях любая из оболочек 9 сухожилий руки может опухнуть и защемить нерв. От длительного пережатия нерв уплощается. Сильно болит запястье. При манипулировании «мышкой» это явление развивается в плечевой и локтевой мышцах. Другими опасными зонами от длительного сидения являются поясница и ноги. Мышцы, находящиеся под воздействием статической нагрузки, не расслабляются, кровообращение в мышечных тканях ухудшается, накапливаются продукты распада (в частности, молочная кислота), в результате возникает боль.

Таким образом, состояние здоровья пользователя ПК может зависеть от таких вредных факторов, как долгосрочное неизменное положение тела, которое приводит к расстройству опорно-двигательного аппарата, постоянное напряжение глаз, воздействие радиации, влияние электростатических и электромагнитных полей, которые могут привести к кожным заболеваниям, головным болям и нарушению функции ряда органов.

Основные нормативные требования для обеспечения безопасной эксплуатации ВТ изложены в санитарных правилах и нормах СанПиН №1.01.004.01 «Гигиенические требования к организации и условиям работы с видеодисплейными терминалами и персональными электронно-вычислительными машинами».

В этом документе содержатся стандарты, устанавливающие критерии безопасности и (или) безвредности, а также требования по обеспечению благоприятных условий для жизни человека. На все ВДТ и ПК должна быть техническая документация и гигиенический сертификат. Определены требования к конструкции этих технических средств, допустимые значения параметров создаваемого ими неионизирующего и ионизирующего излучения.

5.3 Расчет освещённости серверного помещения

Первым делом нам потребуется измерить комнату, для которой рассчитывается освещение, в данном случае это наша серверная, для этого нам нужны следующие параметры: высота, длина и ширина комнаты.

Длина – 5 м. (a)
Ширина – 4 м. (b)
Высота – 3 м. (h)

Площадь помещения равна:

$S = a * b = 5 * 4 = 20$

Следующим шагом по нормативам нам необходимо определить индекс помещения.

$$i = \frac{S}{(h - h1) * (a + b)} = \frac{20}{(3 - 0.8) * (5 + 4)} = 1.01$$

Определение требуемого количества светильников:

$$N = \frac{100 * E * S * K3}{U * n * Фл} = \frac{100 * 400 * 20 * 1{,}25}{48 * 2 * 3100} = 3{,}3$$

$N = 4$ светильника

где:

E — требуемая освещенность горизонтальной плоскости, лк;

S — площадь помещения, м$_2$;

K3 — коэффициент запаса (K3 =1,25);

U — коэффициент использования установки;

$Ф_л$ — световой поток одной лампы, лм;

n — число ламп в светильнике.

Таблица 5.3.2 – Таблица коэффициентов отражения

Поверхность	**Материал**	**Коэффициент отражения, %**
Потолок	Бетон	40
	Штукатурка	73
	Плитка подвесного потолка белая	70
	Плитка подвесного потолка светло-серая	50
Стены	Пластик светлый	60
	Гипсокартон белый	80
	Обои (желтые, бежевые, розовые)	50
	Обои (голубые, светло-зеленые)	30
	Обои (красные, коричневые)	20
Пол	Плитка однотонная светлая	30
	Паркетная доска светлая	20
	Паркетная доска темная	10
	Ламинат светлый (ясень)	30
	Линолеум светло-серый	20
	Ковролин однотонный серый	10

Таблица 5.3.3 – Таблица коэффициента использования

Потолок	80	80	80	70	50	50	30	0
Стены	80	50	30	50	50	30	30	0
Пол	30	30	10	20	10	10	10	0

i=0,6	59	42	35	41	39	35	35	31
i=0,8	66	50	43	48	46	42	41	37
i=1	71	56	**48**	54	51	47	46	42
i=1,25	77	63	54	60	56	53	52	49
i=1,5	80	68	58	63	60	57	56	52
i=2	83	73	62	68	63	61	60	57
i=2,5	86	77	65	71	66	64	63	60
i=3	88	80	68	74	68	67	66	63
i=4	89	83	70	76	70	68	67	64
i=5	91	86	72	78	71	70	69	66

5.4 Расчет защитного заземления

Формула расчёта сопротивления заземления одиночного вертикального заземлителя:

$$R_1 = \frac{\rho}{2\pi L}\left[ln\left(\frac{2L}{d}\right) + 0{,}5\ln\left(\frac{4T+L}{4T-L}\right)\right] = \frac{50}{2*3{,}14*2{,}5} * \left[ln\left(\frac{2*2{,}5}{0{,}045}\right) + 0{,}5 * \ln\left(\frac{4*1{,}75+2{,}5}{4*1{,}75-2{,}5}\right)\right] = 14{,}87$$

где:

ρ – удельное сопротивление грунта (Ом*м),

L – длина заземлителя (м),

d – диаметр заземлителя (м),

T - заглубление заземлителя (расстояние от поверхности земли до середины заземлителя) (м),

π - математическая константа Пи (3,141592),

ln - натуральный логарифм.

Из расчёта следует, что одного стержня будет явно недостаточно, поскольку по требованиям ПУЭ величина нормированного сопротивления составляет Rнорм = 4 Ом (для напряжения сети 220).

Количество электродов определяется методом приближения по формуле:

$$R = \frac{R_1}{K_и * N} = \frac{14{,}87}{(0{,}7*4)} = 5{,}3$$

Таким образом для 6 электродов:

$$Rn = \frac{R_з}{n*\eta} = \frac{14{,}87}{(6*0{,}7)} = 3{,}3\ Ом$$

Таблица 5.4.1 – Удельное сопротивление грунта

Грунт	**Удельное сопротивление грунта, Ом·м**
Торф	20
Почва (чернозем и др.)	50
Глина	60
Супесь	150
Песок при грунтовых водах до 5 м	500
Песок при грунтовых водах глубже 5 м	1000

Таблица 5.4.2 – Таблица значения коэффициента использования

Отношение расстояния между электродами к их длине	**Число электродов**	**Коэф. использования**
1	5	0,7
1	10	0,6
1	15	0,53
1	20	0,5
2	5	0,81
2	10	0,75
2	15	0,7
2	20	0,67

ЗАКЛЮЧЕНИЕ

В дипломном проекте были рассмотрены различные технологии VPN, типы протоколов для построения VPN и виды аутентификаци, проанализированы угрозы информационной безопасности актуальные в период пандемии.

Основной задачей было изучение инфраструктуры предприятия и анализ рисков ее корпоративной сети. Результатом работы стал выбор решения информационной безопасности, ее установка и настройка корпоративной сети. Рассчитана экономическая эффективность внедряемого решения.

Эффективное использование информационных технологий является важным стратегическим фактором повышения конкурентоспособности современных предприятий и организаций. Технология VPN обеспечивает связь между сетями, а также решение различных проблем через безопасный интернет-канал (туннель) между удаленным пользователем и корпоративной сетью.

Исходя из проделанной работы, можно отметить, что основная цель дипломного проекта - анализ и проектирование корпоративной сети – завершена.

СПИСОК ЛИТЕРАТУРЫ

1 Сарычев Д. Бесплатная защита удаленного доступа сотрудников в период пандемии коронавируса (COVID-19) // anti-malware.ru: ООО «AM Медиа». 2020. URL: https://www.anti-malware.ru/ (дата обращения 20.03.2021).

2 Марков А. Информационная безопасность в условиях пандемии COVID-19 // russiancouncil.ru: Российский совет по международным делам (РСМД). 2020. URL: https://russiancouncil.ru/ (дата обращения 20.03.2021).

3 Носов Н. Влияние COVID-19 на информационную безопасность // iksmedia.ru: ООО ИКС Медиа. 2020. URL: https://www.iksmedia.ru/ (дата обращения 20.03.2021).

4 Лахани А. Fortinet: почему социальная инженерия остается главным оружием киберпреступников // itweek.ru: ООО «Издательство СК Пресс». 2021. URL: https://www.itweek.ru/ (дата обращения 21.03.2021).

5 ТОП 5 самых популярных методов социальной инженерии и методы защиты от них // nwu.com.ua: NWU. 2020. URL: https://www.nwu.com.ua/ (дата обращения 20.03.2021).

6 Безмалый В. 5 типов атак социальной инженерии // securitylab.ru: Positive Technologies. 2019. URL: https://www.securitylab.ru/ (дата обращения 20.03.2021).

7 Social engineering // imperva.com: Imperva Sonar. 2020. URL: https://www.imperva.com/ (дата обращения 20.03.2021).

8 A matter of profit: DDoS attacks in Q4 2020 dropped by a third compared to Q3, as cryptomining is on the rise // kaspersky.com: Kaspersky Lab (дата обращения 16.02.2021).

9 Ganti V., Yoachimik O. Network-layer DDoS attack trends for Q4 2020 // cloudflare.com: The Cloudfare Blog. 2021. URL: https://blog.cloudflare.com/ (дата обращения 22.01.2021).

10 Fruhlinger J. DDoS explained: How distributed denial of service attacks are evolving // csoonline.com: IDG Communications, Inc. https://www.csoonline.com/ (дата обращения 12.02.2021).

11 Swinhoe D. Brute-force attacks explained, and why they are on the rise // csoonline.com: IDG Communications, Inc. (дата обращения 20.03.2021).

12 Николахин А.Ю. Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. – 2018. – №3(9). – С. 60-68.

13 J. Mark Jain et al. An efficient approach to secure VPN based on Firewall using IPSec & IPtables // International Journal of Computer Science and Information Technoligies. – Vol. 3(2). – 2012. – P. 3726-3732.

14 Behringer M.H., Morrow M.J. MPLS VPN Security – Cisco Press, 2005. – 312 pp.

15 Reddy K. Building MPLS-based broadcast access VPNs – Cisco Systems, 2004. – 370 pp.

16 Shinder D. Comparing VPN Options // techgenix.com: TechGenix Ltd. 2004. URL: https://techgenix.com/ (дата обращения 20.03.2021).

17 PPTP Client // URL: http://pptpclient.sourceforge.net/ (дата обращения 20.03.2021).

18 Frankel S. et al. Guide to IPSec VPNs. – USA: NIST Special Publication 800-77, 2005. – 126 pp.

19 Baker E. et al. Guide to IPSec VPNs. Revision 1. – USA: NIST Special Publication 800-77, 2020 – 166 pp.

20 Garman J. Kerberos: The Definitive Guide. – USA: O'Reilly &amp Associates, Inc., 2003. – 253 pp.

21 Хромов О. Ю. Организация аутентификации по протоколу «Kerberos» // Молодой ученый. – 2012. – №5(40). – С. 109-112.

22 Velimirovic A. How Kerberos Authentication Works // phoenixnap.com: Global IT services blog. 2020. URL: https://phoenixnap.com/ (дата обращения 20.03.2021).

23 Kerberos authentication // docs.axway.com: Axway documentation. https://docs.axway.com/ (дата обращения 20.03.2021).

24 Афанасьев М. Kerio Control — комплексная безопасность сети // compress.ru: Компьютер Пресс. 2013. URL: https://compress.ru/ (дата обращения 20.03.2021).

25 Мацкевич Д. Требования и рекомендации к серверному помещению // dcnt.ru: Физическая безопасность в ЦОД. 2009. URL: http://dcnt.ru/ (дата обращения 20.03.2021).

26 Безопасность при работе с вычислительной техникой // siblec.ru: Банк лекций. URL: https://siblec.ru/ (дата обращения 20.03.2021).

27 Ю. А. Родичев "Нормативная база и стандарты в области информационной безопасности" - Питер, 2017–256 с.

28 Е. К. Баранова, А. В. Бабаш Информационная безопасность и защита. Учебное пособие - РИОР, Инфра-М – 324 с.