Перевод: английский - русский - www.onlinedoctranslator.com

РУКОВОДСТВО ПО ДИЗАЙНУ

DRACO SIRA - БЕЗОПАСНЫЙ ШЛЮЗ УДАЛЕННОГО ДОСТУПА IP

Когда вам нужно больше, чем сеть для безопасных удаленных сотрудников

УМНЫЕ СТРАТЕГИИ

ДЛЯ УПРАВЛЕНИЯ

ВАШИ ДИСТАНЦИОННЫЕ РАБОТНИКИ

ОГЛАВЛЕНИЕ

УМНЫЕ СТРАТЕГИИ ДЛЯ РАБОТЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ДОМАШНЕГО КОМПЬЮТЕРА 03

СОВЕТ №1 - Обучите своих сотрудников базовым знаниям в области безопасности. 04
СОВЕТ № 2 - Настройте точку доступа VPN для сотрудника, работающего на дому. 05
СОВЕТ № 3 - Разработайте двухуровневую защиту паролем. 06
СОВЕТ №4 - Безопасность USB. СОВЕТ №5 - 07
Персональные устройства. СОВЕТ №6 - Планы 08
резервного копирования. 09

КАК IHSE МОЖЕТ ПОМОЧЬ С ВАШЕЙ СИСТЕМОЙ РАБОТЫ НА ДОМУ 10

ТЕНДЕНЦИЯ В ОБЛАСТИ IP-ПОДКЛЮЧЕНИЙ 10
НЕОБХОДИМОСТЬ УЛУЧШЕННОГО РЕШЕНИЯ ДЛЯ УДАЛЕННОГО IP-ДОСТУПА KVM 12
МАТРИЦА ПРИКРЕПЛЕННАЯ УДАЛЕННАЯ КОНФИГУРАЦИЯ IP 14
РАБОЧИЕ ХАРАКТЕРИСТИКИ ШЛЮЗА УДАЛЕННОГО ДОСТУПА DRACO VARIO SECURE IP 14

ИСПОЛЬЗУЙТЕ СЦЕНАРИИ СЛУЧАИ 15

ЛОКАЛЬНОЕ ПОДКЛЮЧЕНИЕ ЧЕРЕЗ LAN ДАЛЬНЕЕ 15
РАССТОЯНИЕ ПОДКЛЮЧЕНИЕ ЧЕРЕЗ WAN 15

КАК РАЗРАБОТАТЬ KVM-СИСТЕМУ: Главный офис / Удаленный офис 16

ФУНКЦИОНАЛЬНОЕ ОПИСАНИЕ IHSE KVM 17

КЛЮЧЕВЫЕ ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА SIRA 18

СЕТЕВЫЕ РЕШЕНИЯ IHSE SIRA 19

УМНЫЕ СТРАТЕГИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРА ДЛЯ УДАЛЕННЫХ РАБОТНИКОВ

Если вы или ваши сотрудники работаете из дома, вам понадобится этот совет, чтобы обезопасить данные и активы вашей компании.

Удаленные сотрудники представляют собой уникальную проблему для защиты конфиденциальных данных компании, поскольку в удаленных рабочих средах нет таких же мер безопасности, как в офисной среде. Когда сотрудники находятся в офисе, они обычно находятся за несколькими уровнями контроля безопасности и брандмауэрами. Несмотря на то, что в офисной среде могут быть разные уровни безопасности, для компании возникает гораздо больший риск предотвращения нарушений безопасности после того, как компьютер покидает периметр безопасности офиса.

Не существует компании определенного размера, защищенной от кибератак. Кроме того, удаленная работа стала необходимостью для многих организаций, что делает более важным наличие политик безопасности. Сегодня организации по всему миру отправляют сотни тысяч сотрудников домой в ответ на требования к работе на дому в связи со вспышкой COVID-19.

В обычных ситуациях риск безопасности возникает между серверами и компьютерами конечных пользователей. Работа за пределами офисной сети компании теперь добавляет внешних проблем, когда сотрудники получают доступ к данным компании из общедоступного Интернета или домашней офисной сети потребительского уровня. Работа вне офиса добавляет дополнительные проблемы, связанные с доступом к системе, требованиями к пропускной способности и совместным использованием данных.

через несколько точек сети. Теперь это становится гораздо важнее, чем просто периодически менять пароль электронной почты. В то время как компании приспосабливаются к увеличению числа сотрудников, работающих на дому, теперь компании должны помнить о кибербезопасности, чтобы защищать устройства и данные так же, как в офисе.

В свете кризиса COVID-19 многие компании спешат разработать план работы на дому. Хотя у многих из этих компаний было не так много времени на подготовку, практика безопасных онлайн-методов только укрепит дальнейшее функционирование и безопасность вашего бизнеса. Интернет-хакеры и киберпреступники готовы получить доступ к вашим компьютерам, ноутбукам и устройствам Wi-Fi, потому что они знают, что ваши меры безопасности могут быть не такими надежными, как обычно в офисе.

Чтобы помочь нашим клиентам решить самые важные проблемы, связанные с планом работы на дому, мы составили ряд практических советов и рабочих стратегий для минимизации этого потенциального риска - независимо от вертикали вашего бизнеса или его размера.
Эти 6 советов, составленные из лучших ресурсов в Интернете, хотя и не являются полным списком важнейших стратегий, они помогут вам разработать руководящие принципы для разработки ваших стратегий работы на дому.

СОВЕТ №1

ОБУЧАЙТЕ РАБОТНИКОВ С ОСНОВНЫМИ ЗНАНИЯМИ В ОБЛАСТИ БЕЗОПАСНОСТИ

Суть проста: никто в вашей организации не будет заботиться о безопасности данных, защите IP или политике конфиденциальности, пока вы не покажете им, почему это важно, как это влияет на их роли и что они могут сделать для предотвращения кибератак. Следует разработать комплексный план обучения осведомленности о кибербезопасности, чтобы ознакомить сотрудников с общими угрозами, с которыми они могут столкнуться в своей повседневной работе.

Людям, работающим из дома, необходимо дать базовые советы по безопасности: опасаться фишинговых писем, избегать использования общедоступных Wi-Fi, обеспечивать достаточную защиту домашних Wi-Fi-маршрутизаторов и проверять безопасность устройств, которые они используют для получения доступа. работа сделана. Вероятно, что в настоящее время увеличится количество попыток подорвать систему безопасности с помощью фишинговых атак.

Следует особо напомнить сотрудникам, что нельзя переходить по ссылкам в электронных письмах от людей, которых они не знают, а установка сторонних приложений должна выполняться только в добросовестных магазинах приложений, даже на личных устройствах.

Вот некоторые основные проблемы, связанные с угрозами, которые должен понимать каждый работник.

?? Фишинг: Сотрудники должны быть обучены тому, как выявлять и сообщать о фишинге и опасностях взаимодействия с подозрительными ссылками или ввода учетных данных на поддельной странице.

?? Физическая охрана: Требования к физической безопасности могут варьироваться в зависимости от характера организации. Поскольку на предприятиях уже должна быть принята политика физической безопасности, это отличная возможность убедиться, что сотрудники понимают те части политики, которые к ним применяются, например, запирание ящиков стола и правила о допуске гостей в домашний офис.

?? Безопасность рабочего стола: Обозначьте возможные последствия о невозможности заблокировать или выключить компьютеры в подходящее время и подключении неавторизованных устройств к рабочим станциям.

?? Беспроводные сети: Объясните природу беспроводной связи сетей и обозначьте риски подключения к незнакомым.

?? Безопасность паролем: Сложные требования к паролю и побуждение сотрудников к регулярной смене паролей уже должно быть обязательным, но обучение безопасности паролей по-прежнему важно для объяснения рисков, связанных с повторным использованием паролей, использованием легко угадываемых паролей и невозможностью немедленно изменить пароли по умолчанию. Авторизованные инструменты управления паролями также могут быть охвачены

?? Вредоносное ПО: Тренинг по вредоносному ПО должен определить типы вредоносных программ и объясните, на что они способны. Пользователи могут узнать, как обнаружить вредоносное ПО и что делать, если они подозревают, что их устройство заражено.

СОВЕТ №2

НАСТРОЙКА ТОЧКИ ДОСТУПА VPN ДЛЯ СОТРУДНИКА НА ДОМУ

Если ваш сотрудник - новый пользователь, работающий дома, важно предоставить ему безопасный и надежный способ подключения к сетевым системам компании. Один из способов сделать это - использовать виртуальную частную сеть с удаленным доступом (VPN). Услуги VPN обеспечивают дополнительный уровень безопасности, который позволяет скрыть IP-адрес пользователя при шифровании передачи данных и маскировании местоположения пользователя. Вот что вам нужно знать о VPN, если вы планируете воспользоваться этой технологией.

?? Безопасные соединения: Компании используют удаленный доступ VPN для установления безопасных соединений между своими сетями и устройствами, используемыми внештатными сотрудниками. После подключения сотрудники могут получить доступ к ресурсам в сети, как если бы их устройства были физически подключены к ней.

?? Шифрование данных: VPN с удаленным доступом работает создание виртуального туннеля между устройством удаленного сотрудника и сетью компании. Этот туннель проходит через Интернет или другой тип общедоступной сети. Туннель и данные, проходящие через него, защищены протоколами шифрования и безопасности, что обеспечивает конфиденциальность и безопасность данных.

?? Безопасность данных: Использование VPN с удаленным доступом предлагает несколько преимущества для бизнеса. Самым важным преимуществом является безопасность данных. Когда внешние сотрудники отправляют данные через VPN, они шифруются, поэтому, если хакеры захватят данные, они не смогут их использовать.

В более крупных организациях уже есть служба VPN, и им следует убедиться, что у них достаточно рабочих мест, чтобы обеспечить эту защиту для всех своих сотрудников. Небольшим предприятиям может потребоваться назначить поставщика VPN.

Наконец, для некоторых случаев использования вы также можете настроить зашифрованные удаленные подключения к удаленному рабочему столу или другому отдельному серверу. Многие из этих типов подключения (RDP, HTTPS, SSH, виртуальные машины) включают шифрование как часть своего направления обслуживания и не требуют дополнительной VPN или другой службы шифрования для защиты интранзита данных.

СОВЕТ № 3

РАЗРАБОТКА ДВУХУРОВНЕВОЙ ЗАЩИТЫ ПАРОЛЕМ

Практически любая ваша учетная запись в Интернете может быть взломана. После многочисленных широко распространенных нарушений за последние несколько лет технологические компании работали вместе над разработкой стандарта, который оставил бы пароли в прошлом, заменив их более безопасными методами, такими как биометрические или PIN-коды для входа в систему, которые не требуют передачи данных. интернет.

Но пока эти стандарты все еще принимаются, следующий лучший способ защитить ваши учетные записи - это двухфакторная аутентификация или 2FA. Это процесс, который дает владельцу учетной записи вторичный доступ к веб-службам для проверки попытки входа в систему. Обычно это включает номер телефона и / или адрес электронной почты. Вот как это работает: когда вы входите в службу, вы используете свой мобильный телефон, чтобы подтвердить свою личность, щелкнув ссылку в текстовом / электронном письме или введя номер, отправленный приложением для проверки подлинности.

?? Безопасные соединения: Проведите аудит паролей: ваш

Компании необходимо проверить коды доступа сотрудников. Это не означает запроса личных данных людей, но означает, что коды доступа, используемые для доступа к любым корпоративным службам, сбрасываются и переопределяются в соответствии со строгой политикой безопасности. Буквенно-цифровые коды, использование двухфакторной аутентификации должно стать обязательным, и вам следует попросить своих сотрудников применить максимально жесткую защиту на всех своих устройствах. Вы также должны обеспечить надежное хранение всех ваших критически важных для бизнеса паролей на случай, если что-нибудь случится с ключевым персоналом.

?? Настройте двухфакторную аутентификацию: Имея сильную

пароля часто бывает недостаточно, например, если ваши учетные данные просочились в результате утечки данных. Двухфакторная аутентификация (2FA) и двухэтапная проверка (2SV) включают дополнительный шаг для добавления дополнительного уровня защиты ваших учетных записей. Дополнительным шагом может быть подтверждение по электронной почте или текстовым сообщением, биометрический метод, такой как распознавание лица или сканирование отпечатка пальца, или что-то физическое, например USB-брелок.

СОВЕТ # 4

ЗАЩИТА USB

Портативные USB-устройства и мобильные устройства хранения данных играют важную роль в большинстве корпоративных офисов, а также обычно используются в домашних офисах. Однако для такого маленького устройства USB-накопитель может вызвать большие проблемы с безопасностью. Даже если у вас есть надежная политика безопасности конечных точек, сотрудники, не знающие, насколько важно следовать руководствам по безопасности USB, будут использовать эти устройства для копирования как некритичной, так и потенциально конфиденциальной информации для домашнего использования. Обеспечение надлежащей защиты с помощью политики передового опыта и строгого соблюдения обеспечивает значительное снижение риска - и может предотвратить долгие ночи при расследовании утечки данных.

Типичные нарушения компьютерной безопасности легче отследить, но за флешкой труднее следить, особенно после того, как сотрудник покидает рабочий офис. Лучшая политика для рабочих - это *никогда не используйте флешку, если не знаете, откуда она взята* и не продолжайте использовать его, если вы подключили его к системе, за безопасность которой вы не можете честно поручиться.

Если вам необходимо использовать флэш-накопители USB, важно следовать этим простым рекомендациям по обеспечению безопасности USB.

?? Включите функцию USB при необходимости.

Отключите устройства хранения на компьютерах с доступом к конфиденциальной информации. Это ограничит уязвимость и снизит риск передачи несанкционированных данных из вашей организации.

?? Принудительное сканирование USB на всех корпоративных компьютерах всякий раз, когда подключен флэш-накопитель. Это может помочь убедиться, что на диске нет вредоносных или вредоносных программ. Разрешить запуск с накопителя только корпоративных подписанных и одобренных приложений.

?? Если возможно, выдавайте USB-устройствам уникальный серийный номер. числа отмечен в прошивке, а также выгравирован на внешней крышке.

?? Блокировка физических USB-портов на принадлежащих компании компьютеры, используемые для удаленных сотрудников - наиболее радикальный подход - заклеить порты USB лентой с защитой от несанкционированного доступа.

СОВЕТ № 5

ЛИЧНЫЕ УСТРОЙСТВА

Многие предприятия выдают удаленным сотрудникам выделенный портативный компьютер, которым можно централизованно управлять и настраивать в соответствии с внутренними политиками данных, а также защищать с помощью выбранной компанией защиты конечных точек. Однако, если удаленные сотрудники используют собственное компьютерное оборудование из дома, жизненно важно убедиться, что они установили надежные антивирусные инструменты и следуют корпоративным рекомендациям по настройке сети, защите брандмауэра и безопасности паролей.

Если вы работаете в организации с эффективной ИТ-командой, они могут устанавливать регулярные обновления, запускать антивирусное сканирование, блокировать вредоносные сайты и т. Д., И эти действия могут быть прозрачными для сотрудников.

Есть большая вероятность, что работники не следовали тем же протоколам со своими персональными компьютерами, которые являются обязательными на работе. Кроме того, компания, вероятно, может позволить себе более высокий уровень технического контроля, чем сотрудники могут лично. Без них, работающие в фоновом режиме, персональный компьютер не будет безопасным для рабочей информации, потому что он может быть скомпрометирован третьей стороной. По сути, введение персонального компьютера в рабочую сеть, даже удаленно, подвергает риску сеть компании и, возможно, работника, принимая на себя потенциальную ответственность за значительный корпоративный ущерб в результате нарушения политики, практики или того и другого.

?? Использование личных устройств и сетей: Многие рабочие будут вынуждены использовать личные устройства и домашние сети для рабочих задач. Им часто не хватает инструментов, встроенных в бизнес-сети, таких как мощное антивирусное программное обеспечение, настраиваемые брандмауэры и инструменты автоматического онлайн-резервного копирования. Это увеличивает риск попадания вредоносных программ на устройства и утечки личной и служебной информации.

?? Заблокируйте свое устройство Если вам нужно работать в общественных местах пространство, или если вы живете с людьми, с которыми не можете делиться рабочей информацией, важно обеспечить безопасность вашего устройства. Блокировка паролем вашего устройства обычно шифрует его содержимое, пока кто-то не введет пароль.

?? Не используйте рабочие устройства в личных целях: Полегче Сказано - сделано, мы знаем, особенно когда зеркальное отображение этого правила (BYOD, или «Принеси свое собственное устройство») настолько распространено. Тем не менее, точно так же, как во время работы из дома важно проводить границы между работой и семейной жизнью, то же самое можно сказать и о тех устройствах, которые вы используете в этих условиях.

«Убедитесь, что у вас установлено программное обеспечение для защиты от вредоносных программ, чтобы отслеживать активность и не допускать нежелательных злоумышленников. Кроме того, убедитесь, что ваши личные и бизнес-данные хранятся на защищенной платформе, которая шифрует файлы. В идеале ищите платформу, которая имеет встроенные тайм-ауты безопасности, если устройство остается неактивным слишком долго, и позволяет удаленно стереть данные в случае потери или взлома вашего устройства ».

- Брайан Шрейдер, соучредитель и президент BIA

?? Запри свои двери. Если вы принесете свой рабочий компьютер дома или как правило, работают удаленно, конфиденциальная корпоративная информация может оказаться под угрозой. Когда вы приобретаете привычку всегда запирать двери, вы делаете важный шаг на пути к повышению безопасности домашнего офиса. Не подвергайте себя стрессу из-за украденного рабочего компьютера и не навредите своей компании, не выпуская ее данные в открытый доступ.

?? Формализация работы из дома и удаленной работы Политики. Хотя хорошие технологии и политики помогают, правда в том, что именно те сотрудники, которые делают бизнес успешным, являются основным источником риска. Общие правила работы из дома и удаленной работы на компьютере и в Интернете могут помочь, и эти политики можно применять как с помощью технических, так и административных средств контроля.

СОВЕТ № 6

ПЛАНЫ РЕЗЕРВНОГО КОПИРОВАНИЯ - ОБЯЗАТЕЛЬНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ

Резервное копирование данных имеет решающее значение для защиты данных вашей компании и обеспечения непрерывности повседневной деятельности ваших бизнес-процессов. В этой новой домашней среде не достаточно иметь резервную копию на одном настольном или портативном компьютере, если она утеряна или украдена. Компании должны ввести строгие правила в отношении того, как защитить свою интеллектуальную собственность и конфиденциальную информацию. Киберпреступники увеличивают количество атак на удаленный доступ во время кризиса COVID-19, поэтому крайне важно, чтобы удаленные сотрудники были обучены превентивным мерам по резервному копированию информации.

Крайне важно понимать разницу между резервным копированием в локальное хранилище на домашних компьютерах рабочих и полным резервным копированием в офисе компании. Если сотрудники используют свой персональный компьютер для офисной работы, это становится еще одной потенциальной проблемой безопасности. Данные могут быть потеряны разными способами, включая человеческий фактор, физическое повреждение оборудования или кибератаку. Программы-вымогатели или другие типы вредоносных программ могут уничтожить всю систему без возможности восстановления. Компании должны учитывать эти вопросы безопасности, когда разрешают сотрудникам использовать персональные компьютеры или даже компьютеры, предоставленные компанией, расположенные в доме сотрудников или в удаленном офисе.

Следует поощрять сотрудников использовать предоставленные компанией внешние диски или доступ к облачному хранилищу для резервного копирования компьютеров на ежедневной основе. Хотя у работника может быть свой собственный метод резервного копирования для домашнего использования, его не следует использовать для хранения информации компании. Если сотрудник или работник решает уволиться или увольняется, серьезной проблемой становится то, что данные могут быть стерты, утеряны или заражены вирусом. Это всего лишь несколько причин для резервного копирования ваших данных на устройствах хранения, принадлежащих компании. Кроме того, многие из этих систем резервного копирования предлагают множество опций, позволяющих настраивать расписание резервного копирования, которое может отслеживать ИТ-отдел компании.

Если у вашего удаленного работника должны быть USB-накопители для резервного копирования, выпускайте устройства, которые обеспечивают шифрование всего диска и защищены парольной фразой. Это некоторые основные рекомендации, рекомендованные Cyberscount.com.

?? Убедитесь, что для этих дисков есть удаленное управление параметры, такие как удаленная очистка или удаленная блокировка. Выберите диск с инструментами удаленного администрирования, которые также применяют надежные пароли, имеют строгие ограничения на повторный вход и отключают переносимые приложения, а в некоторых случаях самоуничтожаются.

?? Ищите диски, которые обеспечивают регистрацию событий и геотеги, поэтому информация о том, какой компьютер и где сохраняется, сохраняется при каждом использовании.

?? Регулярно проверяйте USB-устройства чтобы только документы в соответствии с допустимым использованием хранятся.

?? Регулярно выполняйте резервное копирование USB-устройств внутри, включая ключи шифрования, для восстановления данных. Убедитесь, что резервные копии надлежащим образом защищены и имеют отдельные процедуры и меры безопасности для резервного копирования ключей шифрования.

?? Процедуры восстановления тестовых данных чтобы гарантировать, что Служба корпоративной безопасности может разблокировать любой USB-накопитель и получить к нему доступ, даже если конечный пользователь или вредоносное ПО злонамеренно отключит USB-накопитель.

?? Знайте свои активы. Получите точное количество USB устройств в вашей организации. Перечислите их по владельцу и использованию. Запретить использование всех персональных USB-устройств, без вопросов, на любых рабочих компьютерах или для любого рабочего использования.

?? Если USB-устройство потеряно, взгляните на последнюю версию защищенного резервное копирование для проверки того, что было потеряно, и потенциального риска. Рассмотрите возможность восстановления диска с помощью этих функций геотегирования, очистки или уничтожения устройства с помощью инструментов удаленного администрирования.

КАК IHSE МОЖЕТ ПОМОЧЬ С ВАШЕЙ СИСТЕМОЙ РАБОТЫ НА ДОМУ

Рисунок 1: Модели модулей безопасного шлюза и удаленного доступа пользователей IHSE SIRA

В IHSE мы всегда ищем способы улучшить производительность наших продуктов, чтобы наилучшим образом удовлетворить ваши потребности в качественном видеоизображении и прозрачном взаимодействии с мышью и клавиатурой. Наши последние модели KVM-удлинителей теперь выводят вас на новый уровень производительности, позволяя операторам беспрепятственно взаимодействовать между нашими KVM-удлинителями в основной полосе частот и переключать продукты через безопасный сетевой интерфейс.

ТЕНДЕНЦИЯ В ОБЛАСТИ IP-ПОДКЛЮЧЕНИЙ

Организации по всему миру используют преимущества IP-технологий для ведения своего бизнеса и общения между персоналом, клиентами и внешними агентствами. Они осознают преимущества и быстро их используют, чтобы повысить эффективность, снизить затраты и повысить гибкость своих повседневных операций.

IP-технология открывает новые возможности для совместной работы и совместной работы предприятий. Люди могут просто и легко подключаться к удаленным компьютерам для доступа к приложениям, которые позволяют им обмениваться данными, управлять сложными данными и контролировать удаленные операции.

Традиционные инструменты на базе IP-сетей доступны уже несколько лет и работают эффективно. Это позволяет операторам, использующим локально установленное клиентское программное обеспечение, управлять совместимыми удаленными серверами. Однако у клиент-серверных решений есть ограничения, которые влияют на их удобство использования. Эти ограничения в основном связаны с динамической производительностью и безопасностью; и то, и другое необходимо учитывать в большинстве профессиональных приложений. Большинство клиент-серверных решений требует дополнительного оборудования, а также установки и настройки сложного программного обеспечения.

Новый защищенный IP-шлюз удаленного доступа (SIRA) от IHSE преодолевает проблемы, связанные с безопасностью, доступностью, оперативностью и качеством изображения традиционного пакетного удаленного IP-соединения с удаленными компьютерами с использованием моделей клиент-сервер. Предпосылка SIRA проста и понятна. Он обеспечивает расширение KVM по IP-сети за счет расширения сигналов клавиатуры, мыши, USB и видеосигнала; таким же образом, как традиционные KVM-удлинители IHSE передают сигналы. Это означает, что удаленный оператор может получить доступ к любому желаемому компьютеру на любом расстоянии, используя клавиатуру и мышь, как если бы они физически находились рядом с этим компьютером.

Предпосылка SIRA проста и понятна.

Он обеспечивает расширение KVM по IP-сети за счет расширения клавиатуры, мышь, USB и видеосигналы; так же, как ИВШЭ традиционный KVM перенос расширителей сигналы.

Рисунок 2: Пример соединений между удаленными точками и локальными соединениями

Сигналы, передаваемые между оператором и компьютером, сохраняют полную целостность, имеют максимально возможную скорость передачи и могут переключаться по запросу. Самое главное, поддерживается полная безопасность системы. Единственные данные, передаваемые по сети, - это визуальные изображения и команды USB. Таким образом, невозможно организовать кибератаки, которые используют операционный контроль над компьютерами или устанавливают вредоносное ПО.

Резервное копирование для сценариев эвакуации

Шлюз SIRA IP не только позволяет сотрудникам продолжать работать наиболее безопасным и эффективным способом, находясь в изоляции дома, но и позволяет выполнять вторичное резервное копирование. объекты, которые должны быть созданы для использования, если первичный центр будет каким-либо образом скомпрометирован. В текущей ситуации это может произойти, когда оператор заболеет, и всю зону управления необходимо эвакуировать и очистить, прежде чем ее можно будет снова использовать.

SIRA может быть включен в существующую систему IHSE KVM или включен как часть удаленного рабочего объекта в качестве расширителя точка-точка; позволяя основным работникам получить доступ к важнейшим системам с полной безопасностью, где бы они ни находились. И убедитесь, что их организация остается работоспособной сейчас и жизнеспособной в будущем.

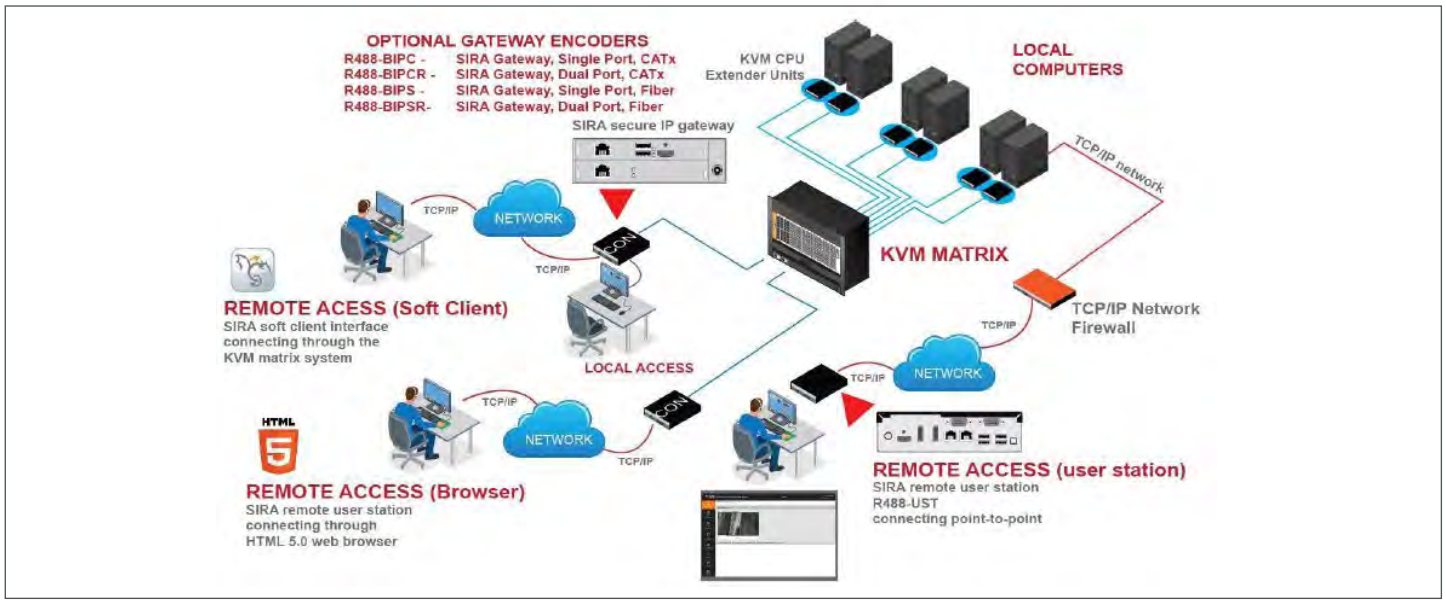


Рисунок 3: Блок-схема соединений для SIRA

IHSE Secure IP Remote Access Gateway (SIRA) надежно и безопасно соединяет удаленного работника

НЕОБХОДИМОСТЬ УЛУЧШЕННОГО РЕШЕНИЯ ДЛЯ УДАЛЕННОГО IP-ДОСТУПА KVM

Пользователям требуется система, которая проста в установке и настройке, гибка в эксплуатации, совместима со всем существующим оборудованием, обеспечивает наилучшую производительность и максимальную безопасность. Тот, который обеспечивает прямой доступ к удаленному компьютеру без задержек и нестабильной производительности, характерных для большинства конфигураций клиент-сервер. Шлюз удаленного доступа Draco vario Secure IP Remote Access Gateway (SIRA) обеспечивает решение этого критически важного эксплуатационного требования. Он работает в двух сферах применения:

?? Автономное удаленное IP-соединение

Выступает в качестве простого решения KVM-удлинителя между одним компьютером или несколькими компьютерами и удаленным пользователем, используя только передачу данных с клавиатуры и мыши по IP-сети. Пользователь может напрямую подключаться к одному удаленному компьютеру или управлять несколькими одновременными сеансами с помощью простого ноутбука или настольного ПК и поставляемого клиентского программного обеспечения.

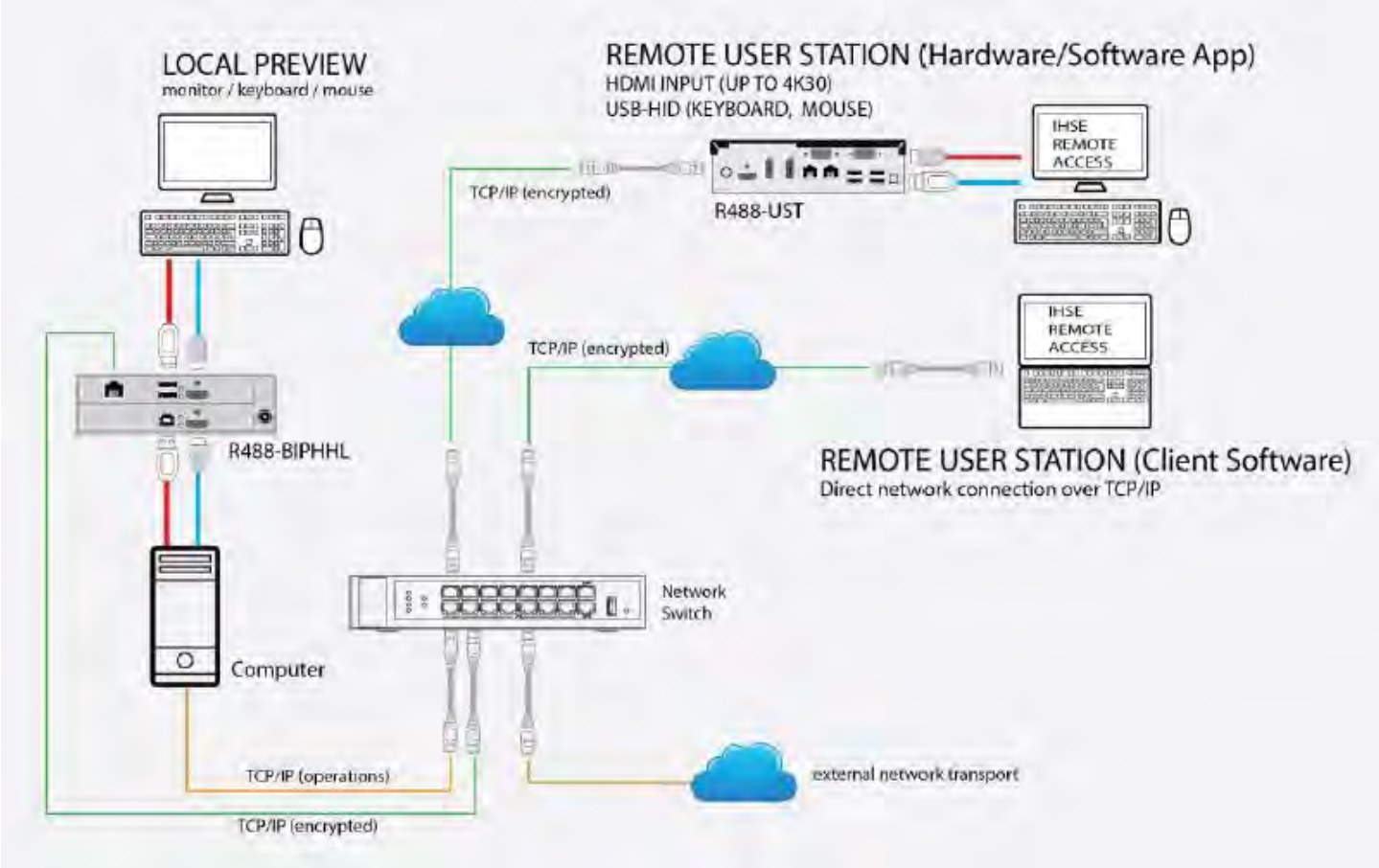


Рисунок 4: Схема подключений для удаленных пользователей в автономном режиме

?? Связь с матрицей KVM

В качестве расширения более крупной системы Draco tera KVM для обеспечения удаленного доступа к коммутатору удаленного пользователя по IP-сети. Эта конфигурация дает пользователю полный подключение ко всем исходным компьютерным устройствам, подключенным к коммутатору Draco tera.

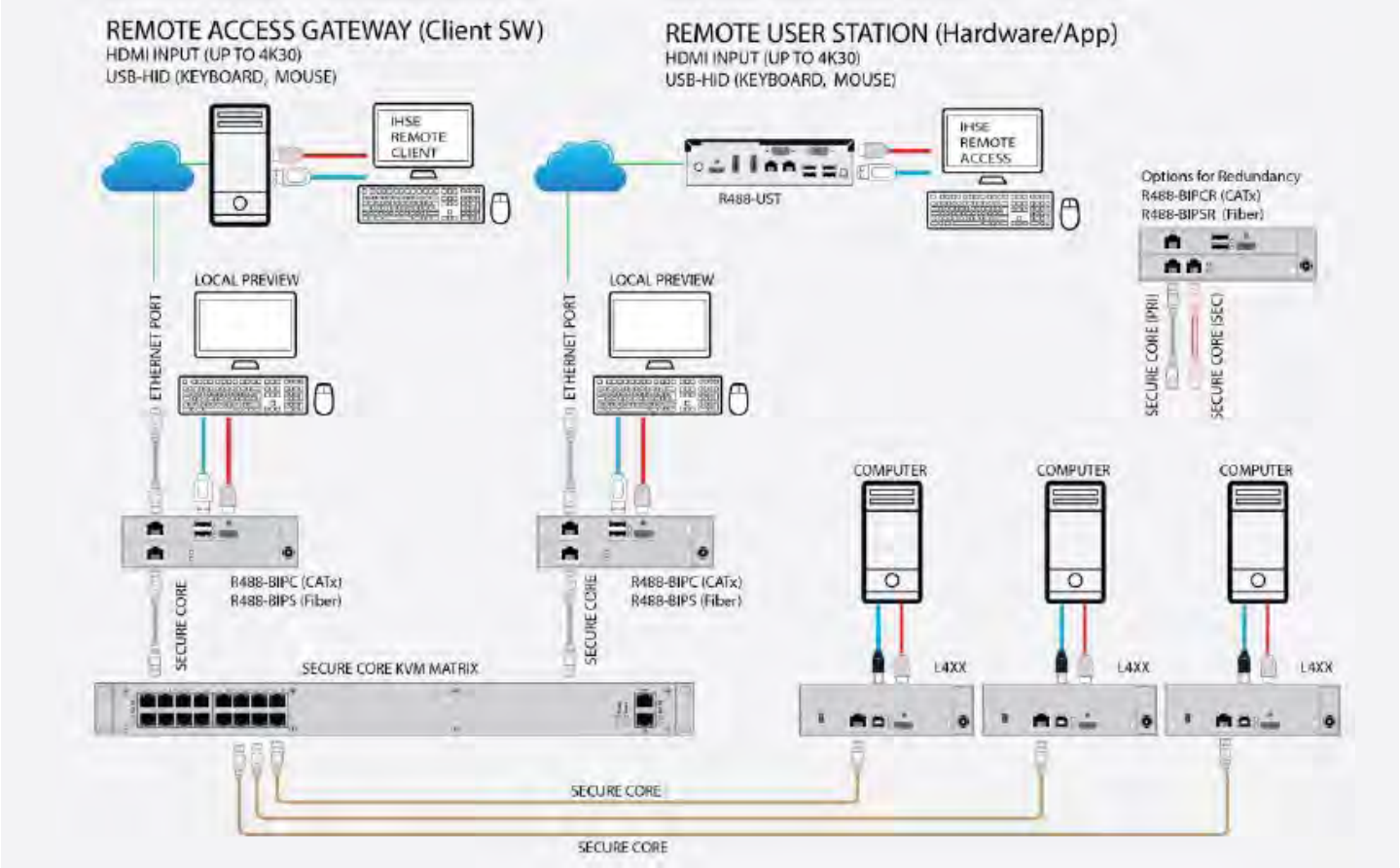


Рисунок 5: Схема подключений для удаленных пользователей для подключения к нескольким источникам

Автономная удаленная IP-конфигурация

SIRA может работать в двух режимах: односеансовый и мультисессионный.

В односессионном режиме компьютер с бесплатным программным клиентом или браузером HTML5.0 действует как декодер, подключенный по IP-сети к кодировщику SIRA, расположенному локально на одном удаленном компьютере. В качестве альтернативы, декодер SIRA K488-UST можно использовать со стандартным видеомонитором, клавиатурой и мышью, не требуя дополнительного компьютера и программного клиента.

В многосеансовом режиме декодер SIRA K488-UST обеспечивает удаленный доступ к нескольким отдельным компьютерам в виде мозаики по IP-сети. Декодер SIRA может отображать несколько источников на одном дисплее с использованием четырехуровневого разделения или раскладки изображения «картинка в картинке». Изображения можно размещать и дублировать на нескольких пользовательских мониторах. Взаимосвязь и передача информации в основном осуществляется на уровнях компьютерного видео, USB и звука с использованием сигналов, выводимых из периферийных портов компьютера и вводимых в них.

В отличие от традиционных конфигураций клиент-сервер нет необходимости в дополнительном программном обеспечении на клиентских или серверных устройствах. Вся трансляция и передача сигналов производятся в устройствах кодирования и декодирования SIRA.

Во время работы пользовательская консоль, состоящая из видеоэкрана, клавиатуры и мыши, действует так, как если бы она была напрямую подключена к соответствующим портам пользовательского интерфейса компьютера. Оператор имеет прямое управление компьютером с помощью собственной клавиатуры и мыши.

Автономное решение поддерживает транспорт виртуальных носителей (VM), который позволяет подключать USB-устройства, включая портативные карты памяти, CD-ROM, NAS и другие устройства хранения, как на стороне сервера, так и на стороне пользователя канала передачи. Файлы можно передавать в обоих направлениях. В целях безопасности и контроля системный администратор устанавливает права пользователей на эту функцию и управляет ими.

УДАЛЕННАЯ IP КОНФИГУРАЦИЯ С МАТРИЦЕЙ

SIRA предоставляет удобный и высокоэффективный метод удаленного подключения к существующей коммутационной инфраструктуре KVM. Цель этой конфигурации - дать возможность удаленному пользователю взаимодействовать со всеми компьютерами в инфраструктуре KVM с прямым подключением, как если бы они физически находились рядом с ней. Пользователю могут быть предоставлены те же права доступа и возможности доступа ко всем компьютерам в сети, что и ассоциированному лицу, подключенному непосредственно к KVM-переключателю. Как и в случае с автономным решением, установка дополнительного программного обеспечения на клиентские или серверные устройства не требуется. Все процессы трансляции и передачи сигналов выполняются в устройствах кодирования и декодирования SIRA или клиентском программном обеспечении, которое работает как портативное приложение без установки программного обеспечения.

Во время работы пользовательская консоль видеоэкрана, клавиатуры и мыши действует так, как если бы они были напрямую подключены к соответствующим портам пользовательского интерфейса компьютера. Отдельные пользователи не ограничены одной удаленной установкой KVM и могут иметь доступ к нескольким KVM-переключателям в разных местах, снабженных локальным кодировщиком SIRA.

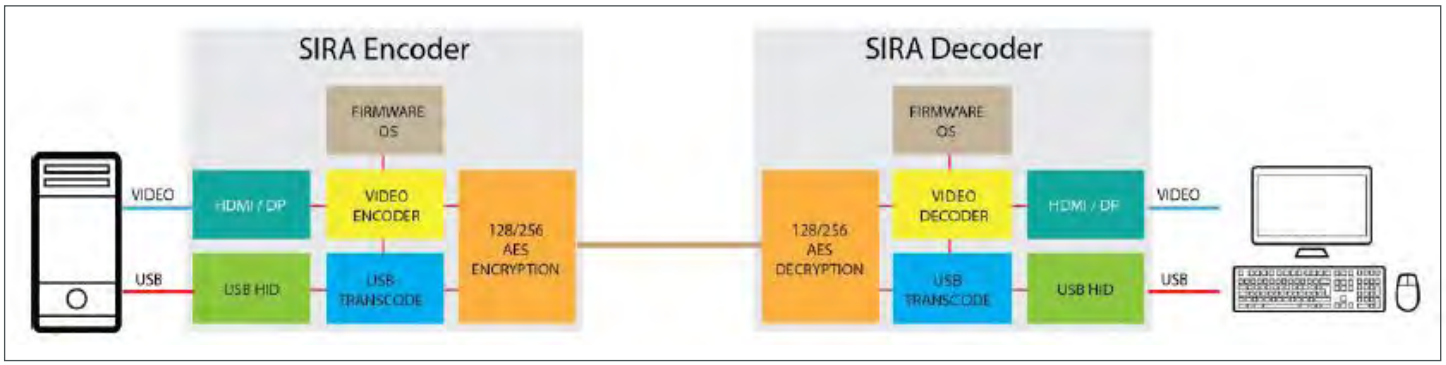


Рисунок 6: Схема подключения сигналов между кодером и декодером

РАБОЧИЕ ХАРАКТЕРИСТИКИ ШЛЮЗА УДАЛЕННОГО ДОСТУПА DRACO VARIO SECURE IP

ВИДЕО И ПЕРЕДАЧА ПО USB

Видеосигналы, полученные от удаленного компьютера, принимаются и обрабатываются собственным кодеком в кодировщике SIRA, который эффективно управляет сжатием и передачей изображений через IP-сети.

Процесс передачи видеосигнала работает следующим образом:

?? Кодировщик шлюза удаленного доступа Draco Secure IP предоставляет только фиксированную информацию EDID для видеокарты хост-систем. Нет обратного канала для передачи данных с видеокарты на кодировщик и далее удаленному пользователю.

?? Захват видео с вывода главного ПК на компьютер видеопорт графической карты не передается в виде необработанных данных на удаленный клиент. Он обрабатывается и, следовательно, обрабатывается и отправляется по сети в полностью зашифрованном виде с использованием ключей RSA 2048 и выбираемого шифрования AES 128/256.

?? Биты видеоданных передаются в виде сжатого потока. посредством непрерывного захвата отдельных снимков экрана или смены кадров (межкадровое сжатие) для экономии полосы пропускания.

?? Данные USB транслируются на обоих концах передачи. канал для передачи в обоих направлениях между блоками кодирования и декодирования SIRA для завершения подключения к USB-портам компьютера и устройствам USB-HID.

ДОСТУП И ПРАВА ПОЛЬЗОВАТЕЛЯ

Пользователь может получить безопасный доступ к удаленному компьютеру вплоть до уровня BIOS исходного ПК без какого-либо специального программного обеспечения или драйверов. Активная связь с исходным ПК через кодировщик и декодер SIRA устанавливается только по запросу пользователя. Если соединение не установлено, данные KVM не передаются в сеть.

Операторы, использующие SIRA для доступа к удаленным компьютерам, могут быть ограничены в их функциональных возможностях (например, доступ только к видео, блокировка определенных определенных символов клавиатуры и т. д.). Это основано на профилях пользователей, описывающих варианты доступа.

СООБРАЖЕНИЯ БЕЗОПАСНОСТИ

Система SIRA позволяет стандартную клавиатуру, мышь и передачу видеосигнала, а также передачу данных через USB-накопитель при строгом контроле доступа. Они защищают от кибератак, предотвращая доступ хакеров к хост-системам.

Доступ к операционной системе шлюза удаленного доступа Draco Secure IP или управление ею с помощью этих интерфейсов невозможно, поскольку кодировщик обрабатывает только сигналы клавиатуры и мыши. Конфигурация операционных систем SIRA отделена от пользовательского интерфейса и недоступна.

Кроме того, операционная система SIRA основана на прошивке. Для смены ОС требуется перезагрузка блока SIRA. Операционная система SIRA защищена зашифрованной подписью, один раз для защиты интеллектуальной собственности кодировщика, а второй раз для предотвращения любых манипуляций со стороны третьих лиц.

ИСПОЛЬЗУЙТЕ СЦЕНАРИИ СЛУЧАИ

ЛОКАЛЬНОЕ ПОДКЛЮЧЕНИЕ ПО ЛВС

Типичное приложение: подключение к одиночным компьютерам или компьютерам, подключенным к матрице, внутри здания, на месте или в кампусе для обеспечения удобного доступа, физического разделения операторов или создания резервных или аварийных конфигураций.

ДАЛЬНЕЙШЕЕ ПОДКЛЮЧЕНИЕ ЧЕРЕЗ WAN

Подключение к глобальной сети между удаленными точками, например, для работы дома или аварийного восстановления.

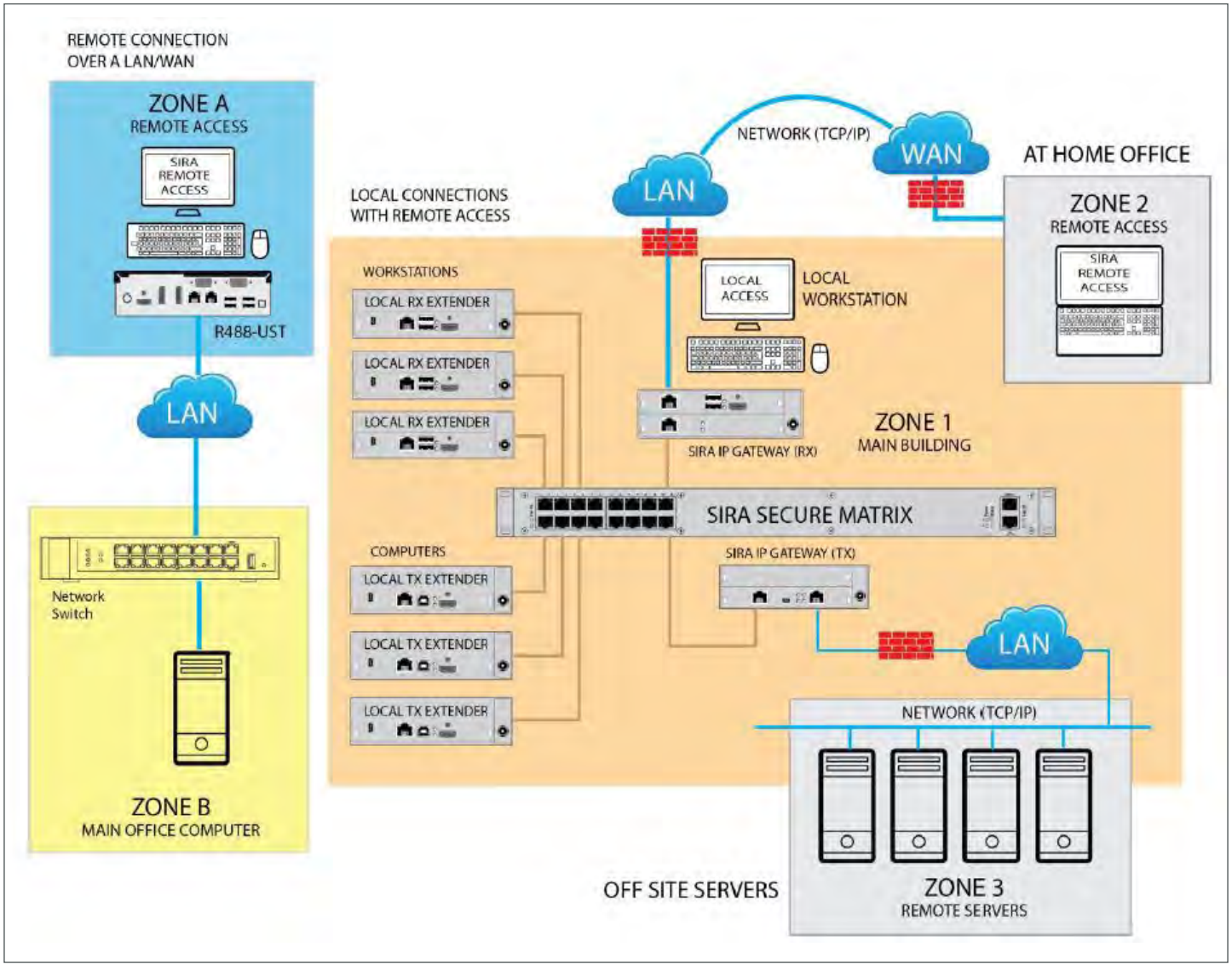


Рисунок 7: Обзор возможностей подключения для систем KVM SIRA

КАК РАЗРАБОТАТЬ KVM-СИСТЕМУ: ГЛАВНЫЙ / УДАЛЕННЫЙ ОФИС

Факторы, которые следует учитывать при разработке защищенной IP KVM-системы для работы дома.

Важно тщательно продумать наиболее подходящие компоненты KVM для вашего конкретного приложения и требований. Чтобы помочь найти лучшее решение, вам следует начать с некоторых основ, чтобы составить список необходимых материалов. Вот несколько важных вопросов, на которые стоит обратить внимание:

?? Существующие настройки общего доступа к компьютеру

- Определите количество компьютеров или серверов, которыми вы хотите поделиться сейчас, и то, что, по вашему мнению, может понадобиться в будущем.
- Какие периферийные устройства (клавиатура, мышь, трекболы, аудио и т. Д.) Будут подключены к компьютерам?
- Определите количество пользователей, которым потребуется доступ извне и внутри.
- Скольким пользователям потребуется доступ как с внешних, так и с внутренних рабочих станций?
- Сколько пользователей должны будут иметь доступ к нескольким компьютерам одновременно?

?? Требуемый формат видео

- Какие видеоинтерфейсы нужно подключить. (DVI, HDMI, DisplayPort, VGA)
- Какие разрешения видео нужно поддерживать?

?? Типы подключения и расстояния

- Будете ли вы использовать виртуальную частную сеть (VPN) через LAN или WAN?
- Какое расстояние между устройствами в корпоративном офисе?
- Вам потребуются кабели 5e / 6/7 или оптоволоконные соединения?

?? Безопасность и защита данных

- Какой тип защиты паролем и шифрования будет использоваться для соединений на работе из дома?
- Будет ли LDAP или активный каталог использоваться для управления входом пользователя в систему?
- Какой тип системы резервного копирования или резервирования будет включен?

Если вам нужна помощь, чтобы решить, какая система KVM лучше всего подойдет для вашей конфигурации, свяжитесь с нашей группой технического проектирования по адресу info@ihseusa.com. Мы можем помочь с рекомендациями, предложениями или особенностями, которые следует учитывать при покупке KVM для работы на дому.

IHSE USA LLC
1 корпоративный диск
Крэнбери, Нью-Джерси 08512
Соединенные Штаты Америки
Тел .: +1 (732) 738 878 0
info@ihseusa.com
www.ihseusa.com

ФУНКЦИОНАЛЬНОЕ ОПИСАНИЕ IHSE KVM

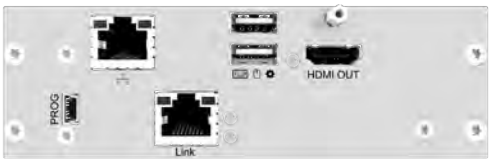
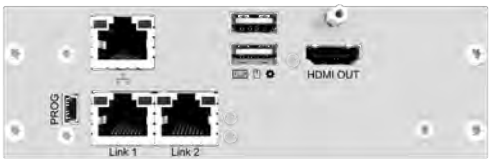
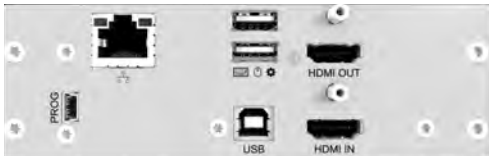
Теперь, когда вы знаете, что создавать, следующая часть - выяснить, какие типы компонентов потребуются для настройки вашей системы KVM.

МАТРИЧНАЯ СИСТЕМА SIRA KVM (КЛАВИАТУРА, ВИДЕО, МЫШЬ) СОСТОИТ ИЗ ЭТИХ ОСНОВНЫХ ЧАСТЕЙ:	
Тип устройства	**Определение**
?? Расширитель, передатчик (ЦП)?? для местных подключений?? Точка-точка или матричный переключатель?? Доступен в оптоволокне или CAT X	Передающее устройство-расширитель (ЦП), соединяющий исходные устройства, такие как сервер, компьютер или видеокамеры. От устройства ЦП один разъем RJ-45 (медный) используется для распространения передаваемого сигнала данных от источника на входы матричного переключателя или непосредственно на приемное устройство (CON). Типичные подключаемые сигнальные устройства включают HDMI, DVI, VGA, USB, аудио и RS-232.
?? Удлинитель, приемник (CON)?? Для местных подключений?? Точка-точка или матричный переключатель?? Доступен в оптоволокне или CAT X	Устройство-расширитель приема сигнала (CON), принимающее один разъем RJ-45 (медный) для приема тракта данных от ЦП или матричного коммутатора. К устройству CON подключаются дисплеи, интерфейсные устройства или записывающие устройства для создания графических изображений, USB-соединений, аудио-соединений и последовательной передачи данных.
?? Матричный переключатель KVM?? Доступен в оптоволокне или CAT X	Матричный коммутатор (MS) позволяет подключать устройства CPU и CON к централизованному методу распределения для совместного использования, переключения и управления большим количеством устройств из одной точки. Матричным переключателем можно управлять с помощью горячих клавиш клавиатуры, апплета Java Tool или через стороннюю систему управления через API.
?? Безопасный IP-шлюз	Устройства кодирования и декодирования сигналов, соединяющие удаленного пользователя с физической системой KVM через LAN или WAN соединение.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА SIRA

SIRA ПРЕДОСТАВЛЯЕТ ПОЛЬЗОВАТЕЛЯМ СПИСОК ПРЕИМУЩЕСТВ:	
Прямое подключение к автономным компьютерам Непосредственно подключайте удаленные компьютеры в световых средах с централизованным удаленным управлением распределенными компьютерами.	**Подключение удаленной матрицы KVM** Удаленное подключение к матричным системам Draco tera KVM через локальные и глобальные сети TCP / IP. Идеально подходит для резервных сценариев и резервных операций.
Управляйте удаленными компьютерами до уровня BIOS Подключение через внешние видео и USB-порты. На хостах не нужно устанавливать программное обеспечение или драйверы.	**Высокая производительность** Встроенная поддержка видео 4K30 и встроенный 16-битный звук. Подключение к сетям 4K60 Draco tera со встроенным преобразователем частоты кадров.
Легкость установки Не требует установки программного обеспечения или драйверов. Использует Windows и клиент на базе Java для Linux, Mac. Вариант браузера HTML5.0.	**Низкая сложность IP** Ограниченные требования к пропускной способности данных. Нет многоадресной рассылки. Никаких настроек IGMP и конфигураций jumbo-фреймов. SIRA предназначен для использования в сетях дальней связи (WAN), а также в сценариях LAN и CAN.
Безопасный Включает двухуровневую аутентификацию при входе в систему: доступ SIRA и Draco tera. Маскировка IP-адресов для диапазона IP-адресов и индивидуальных уровней IP-адресов. Ключ RSA2048, шифрование AES256-бит. Контроль доступа администратора.	**Максимальное сопротивление кибератакам** Система работает с использованием команд клавиатуры и мыши без доступа к файловой системе ПК или ОС через IP-сеть.
Варианты надежности и резервирования Резервный источник питания и варианты конфигурации порта связи.	**Внеполосная работа** Прямое управление матрицей с помощью нажатия клавиш и экранного меню. Резервный и отказоустойчивый режим работы.

СЕТЕВЫЕ РЕШЕНИЯ IHSE SIRA

НОМЕРА ДЕТАЛЕЙ		
	**R488-BIPC**	Secure IP Gateway, CON Module, Cat-X, для разрешений до 3840X2160 при 30 Гц , локальный KVM-выход, 2X USB, HDMI, RJ-45 для 1G LAN, RJ-45 для KVM-канала длиной до 140 м через IHSE Secure Core Link.
	**R488-BIPCR**	Secure IP Gateway, CON Module, Cat-X, для разрешений до 3840X2160 при 30 Гц , локальный KVM-выход, 2X USB, HDMI, RJ-45 для 1G LAN, RJ-45 для KVM-канала длиной до 140 м через IHSE Secure Core Link. Резервные порты Secure Core для соединений с замкнутым контуром
	R488-BIPS	Безопасный IP-шлюз, модуль CON, оптоволокно, для разрешений до 3840X2160 при 30 Гц , локальный KVM-выход, 2X USB, HDMI, RJ-45 для 1G LAN, LC Duplex для KVM-канала длиной до 10 км через IHSE Secure Core Link.
	R488-BIPSR	Secure IP Gateway, CON Module, Cat-X, для разрешений до 3840X2160 при 30 Гц , локальный KVM-выход, 2X USB, HDMI, RJ-45 для 1G LAN, RJ-45 для KVM-канала длиной до 140 м через IHSE Secure Core Link. Резервные защищенные основные порты для соединений с замкнутым контуром. Резервные порты Secure Core для соединений с замкнутым контуром
	**R488-BIPHL**	Безопасный IP-шлюз, соединения точка-точка, с разрешением до 3840X2160 при 30 Гц , локальный KVM-выход, 2X USB, HDMI, RJ-45 для 1G LAN. Матрица совместима с добавленными компонентами.
	K488-СТЮ	KVM EXTENDER, IP, пользовательская станция удаленного доступа, видео до 4K30, USB-HID, аудио, RS232

HOWHIGH - ПРОИЗВОДИТЕЛЬНОСТЬKEYBOARDVI DEOMOUSE
РАСШИРЕНИЕ И ПЕРЕКЛЮЧЕНИЕТ ECHNOLOGYENABLESIMPRO
VEDPRODUCTIONWORKFLOW SANDPRISTINEVIDEODISP LAY

IHSE GmbH
Штаб-квартира
Benzstr. 1
88094 Oberteuringen
Германия

Тел .: +49 (7546) 9248-0
info@ihse.de
www.ihse.de | www.ihse.com

IHSE USA LLC
1 корпоративный диск
Крэнбери, Нью-Джерси 08512
Соединенные Штаты Америки

Тел .: +1 (732) 738 878 0
info@ihseusa.com
www.ihseusa.com

IHSE GmbH Asia Pacific Pte Ltd
158 Kallang Way, # 07-13A
Сингапур 349245

Тел .: +65 (6841) 470 7
info-apac@ihse.com
www.ihse.com | www.ihse.com.cn

IHSE China Co., Ltd.
Комната 814, дом 3, улица
Кечжу № 233, район Хуанпу
Гуанчжоу КНР

Тел .: +86 (189) 888 381 11
info@ihse.com.cn
www.ihse.com.cn