

Совместная работа на основе политик. Переход к единой корпоративной инфраструктуре для уверенного сотрудничества и взаимодействия.

Обзор рассматриваемых вопросов

Деловой мир переживает стремительные перемены. На пути от множества разрозненных региональных экономических систем к единой взаимосвязанной мировой экономике решающее значение имеют скорость и гибкость. Организации активно отказываются от практики физических встреч и конференций в пользу виртуальных контактов, используя развитые сетевые инструменты, позволяющие сотрудникам преодолевать границы регионов и часовых поясов. Совместно работая с коллегами, партнерами, поставщиками и заказчиками, люди стремятся уменьшить затраты, использовать базы знаний для оперативного принятия решений, повысить продуктивность работы, ускорить внедрение инноваций и выход на рынок. В условиях повсеместного распространения широкополосного доступа сформировалась технологическая база, необходимая для подобного качественного скачка. Сотрудники выбирают мобильность благодаря появлению устройств и сетей, позволяющих работать в таком формате. Становление сервис-ориентированной архитектуры (SOA) закладывает основу для ускорения новаторства в сфере программного обеспечения, в то время как растущее распространение концепции «ПО как услуга» (SaaS) обещает сделать эти решения доступными значительно более широкому контингенту квалифицированных сотрудников.

Насущная необходимость достигать результатов быстрее, эффективнее и с меньшими затратами мотивирует компании всех размеров и во всех отраслях предусматривать возможности совместной работы во всех бизнес-процессах и организационных процессах с участием как внутренних, так и внешних сторон. Предприятия отмечают, что возможность эффективно включать в свои процессы заказчиков, партнеров, поставщиков, производителей и другие внешние стороны позволяет ускорить выход на рынок, сократить цикл продаж, повысить результативность всех рабочих процессов и достигнуть более высокого уровня лояльности и удовлетворенности клиентской базы. Однако оборотной стороной этих преимуществ являются риски. Интернет не только предоставил рассредоточенным рабочим группам прозрачный совместный доступ к данным и ресурсам, но и открыл взломщикам возможность перехвата этих данных на пути к адресату, а также эксплуатации уязвимостей в каналах совместной работы для получения несанкционированного доступа к важным данным и сетевым ресурсам. Принимая решение об организации совместной работы через Интернет, нельзя упускать из виду эти проблемы, поскольку для большинства организаций информация является наиболее ценным активом и залогом жизнеспособности бизнеса.

По-настоящему эффективное решение для совместной работы на основе политик позволяет свободно организовывать взаимодействие любого круга участников в любой момент в реальном времени с асинхронным совместным использованием структурированных или неструктурированных информационных материалов независимо от их местоположения. Развитая система политик наделяет сеть возможностью различать контекстные атрибуты различных пользователей и ресурсов для принятия точных решений об информационных объектах, доступных пользователям, и об их допуске в сетевые совместные рабочие пространства.

В этом документе освещено развитие механизмов совместной работы, текущее состояние размещаемых у заказчика и доступных по требованию средств взаимодействия и обоснована принципиальная значимость политик в обеспечении защищенного межкорпоративного информационного взаимодействия и выполнении нормативных требований. Кроме того, в данном документе акцентируется внимание на уникальном положении компании Cisco в отрасли

и поясняется, каким образом этот статус помогает компании решать стоящие перед заказчиками задачи, создавая уверенные возможности совместной работы в любой сети и на любом устройстве. Рассматриваемая концепция совместной работы на основе политик позволяет соединить лучшее из двух сфер: соблюдение самых строгих требований информационной безопасности и нормативно-правовых актов при предоставлении пользователям возможности настраивать и персонализировать свои рабочие пространства по аналогии с личными и социальными пространствами в Интернете.

Введение

Распространение Интернета и широкополосных сетей привело нас в мир постоянного присутствия в сети и доступности ресурсов по запросу, заложив основу коммуникационной среды глобального взаимодействия. Вместе с тем, совместная работа в бизнесе чаще всего не подразумевает взаимодействия лицом к лицу или физического присутствия в одном помещении. Благодаря все более и более развитым IP-сетям, приложениям и оконечным устройствам взаимодействие происходит при помощи IP-телефонии (VoIP), web- и аудиоконференций, электронной почты, мгновенного обмена сообщениями, средств мобильности и видеосвязи. Такая возможность сотрудничества в виртуальном формате ускорила динамику бизнеса и принесла с собой существенные преимущества: объединение разнородного штата, повышение уровня мобильности и новаторства, увеличение производительности, уменьшение затрат, сокращение сроков выхода на рынок и окупаемости.

Концепция совместной работы радикально переопределила глобальную конкурентную среду. Наличие инструментов взаимодействия с важнейшими деловыми партнерами, адаптированных для нужд предприятий среднего размера, может быть решающим фактором конкурентоспособности, особенно по сравнению с крупными глобальными корпорациями, для которых сдерживающим фактором является неспособность оперативно принимать решения и действовать достаточно быстро.

Кроме того, как никогда прежде, корпорациям для роста требуется более широкий доступ к новым заказчикам, улучшение существующих отношений, завоевание новых рынков и освоение новые бизнес-моделей. Глобализация заставляет компании конкурировать на большем числе рынков, привлекая все более мобильный и рассредоточенный персонал. Хотя инструменты дистанционной совместной работы становятся общепринятыми, политики безопасности и технологии защиты совместно используемой информации не всегда реализуются должным образом, создавая для компаний осязаемые юридические и финансовые риски.

Почему совместная работа является критическим фактором успеха для предприятия?

Объединяя самые различные круги персонала и предлагая инструменты взаимодействия с важнейшими деловыми партнерами, концепция совместной работы приобрела решающее значение для предприятий, заинтересованных в быстром росте и сохранении конкурентоспособности. Например, профессионалы в сфере продаж могут улучшить свои показатели, выстраивая отношения для наращивания объемов реализации существующим покупателям, расширения клиентской базы, освоения новых каналов и ускорения закрытия крупных сделок. Отделы продаж должны использовать весь арсенал доступных средств для завоевания заказчиков и не могут позволить себе ждать, пока компания налаживает процессы совместной работы. В отсутствие защищенных механизмов связи они все равно будут обмениваться информацией, надеясь обойтись без неприятностей. Это реальные проблемы, которые могут быть решены за счет совместной работы на основе политик. Теперь организации могут реализовать политики контроля и управления информацией в своих сетях и устройствах, не дожидаясь, когда их критические данные окажутся под угрозой.

Компании, ведущие коммерческую деятельность в Интернете, также используют механизмы совместной работы в своих интересах. Для многих организаций, занимающихся продажей конкурирующих товаров или услуг через Интернет, уровень сервиса часто является основным

конкурентным дифференциатором. Когда возникают проблемы с обслуживанием заказчиков, оперативность разрешения ситуации имеет критическую значимость для сохранения позиций на рынке. Заказчика не удовлетворит объяснение, что файл не смог преодолеть межсетевой экран из-за настройки несовместимой политики. Обслуживание заказчиков показывает, что средства безопасности для совместной работы должны не только защищать интеллектуальную собственность, но и обеспечивать ведение бизнеса, иначе они создадут больше проблем, чем смогут решить.

Сегодня инструменты, помогающие справиться с этими задачами, все чаще встречаются в корпоративном коммуникационном инструментарии. Стратегическое применение совместной работы в реальном времени позволяет повысить производительность, принимать решения в более сжатые сроки, ускорить выход на рынок, получить доступ к экспертам везде и в любое время, а также повысить лояльность заказчиков и поставщиков. Все эти факторы будут способствовать росту и повышению рентабельности, делая совместную работу на основе политик фундаментом глобальных экономических отношений.

По мере того как сети все дальше выходят за физические пределы организаций, такие аспекты, как безопасность и конфиденциальность, целостность информации, качество обслуживания (QoS), доступность и надежность, будут играть все более важную роль в обеспечении защищенной совместной работы предприятий и их экосистем.

Проблемы совместной работы

На истинно безграничном предприятии платформа совместной работы на основе политик предложит развитые средства взаимодействия с пользователем, которые поднимут на новый уровень все аспекты бизнеса. Конвергентные сети могут стать каналами, по которым удаленные работники внутри или вне периметра традиционной сети будут обмениваться критически важной информацией с независимыми подрядчиками, участниками товарной цепочки и заказчиками, а также более широкой экосистемой партнеров. Но объединение этих коммуникационных каналов на базе единой защищенной платформы все еще представляет огромную проблему. Например, необходимо состыковать в сети старое оборудование и приложения множества различных поставщиков, получить доступ к данным на изолированных объектах и скрыть детали реализации за практичным интерфейсом, не требующим или почти не требующим обучения пользователей.

Однако без прочных корпоративных политик и всестороннего решения по управлению политиками наиболее ценный актив организации – ее информация – может оказаться под угрозой. По данным Координационного центра противодействия хищению личных данных (Identity Theft Resource Center, ITRC), за 2007 г. в руки злоумышленников могли попасть 127 млн записей данных. Анализ, проведенный Ponemon Institute, независимым исследовательским агентством в сфере защиты личных данных, показал, что нарушение защиты одной записи данных в 2007 г. в среднем обходилось предприятиям США в 197 долл.

Для защиты бесценных бизнес-активов, как локально, так и в электронных сетях, и исключения критических точек отказа требуется всесторонняя архитектура на основе политик. Решение для динамического анализа действий позволяет более детально реализовать управление доступом в инфраструктуре.

Эффективный подход к проблемам безопасности на основе политик

Особенностью сегодняшней деловой среды является множество нормативных требований, которые чрезвычайно сложны и специфичны для разных юрисдикций. Объединив традиционную защиту периметра с более тонкой стратегией для технологий совместной работы, организации получают возможность эффективно выполнять требования безопасности и конфиденциальности, диктуемые следующими нормативно-правовыми актами: законом Сарбейнса-Оксли; законом Грэма-Лича-Блайли (GLB); законом о передаче страховых данных и отчетности медицинских учреждений (HIPAA); стандартом защиты данных в отрасли платежных карт (PCI); европейской конвенцией Базель II и т. п.

Но даже с защитой периметра и стратегиями для технологий совместной работы нельзя ручаться за полную неуязвимость сети. Например, веерные атаки, при которых эксплуатируется самое слабое звено в инфраструктуре унифицированных коммуникаций, могут поразить и другие элементы сетевого окружения. Объектами атак часто становятся карманные мобильные устройства. Так взломщики пытаются обойти более прочную защиту других вычислительных устройств типа ноутбуков. Чтобы защитить мобильные устройства от веерных атак и других потенциальных угроз, организациям необходимо свести политики безопасности беспроводной сети в укрупненную стратегию политики безопасности.

Объединение политик безопасности помогает обеспечить соответствие нормативным требованиям и защиту ценных корпоративных активов, но при этом является лишь частью стратегии защищенной совместной работы. Для уверенной совместной работы и обеспечения целостности информации и доступности ресурсов организациям необходимы действенные механизмы управления данными и доступом к ним пользователей. Инструменты управления идентификационными данными помогают организациям управлять пользователями, группами, ролями и атрибутами. Например, с помощью этих инструментов можно разрешить доступ только к определенному набору данных исходя из роли пользователя в организации. Аналогичным образом инструменты классификации данных помогают руководителям отделов ИТ на предприятиях при анализе типов и ценности информации, пересылаемой по каналам совместной работы. В свою очередь, на основе этих сведений они могут определить конкретный круг пользователей, групп и ролей, которым разрешен доступ к данным. Инструменты управления идентификационными данными и классификации данных должны работать параллельно и по возможности должны быть интегрированы в инфраструктуру управления политиками для расширения функциональности корпоративной сети как защищенной платформы для совместной работы.

Примеры выгодного применения стратегии на основе политик в различных отраслях

Если совместная работа и безопасность на сетевом уровне представляют критическую значимость для бизнеса, то управление политиками и применение политик столь же важны как часть сетевой структуры. С практической точки зрения функции безопасности должны быть стандартизованными, простыми в управлении, прозрачно интегрированными в платформу совместной работы, недорогими с точки зрения развертывания и управления, совместимыми с разными технологиями и платформами и достаточно расширяемыми для адаптации к специфике потребностей каждой компании. В то же время организации должны реализовывать управление политиками в контексте потребностей бизнеса, определяя цели, роли и сценарии пользования для всех приложений, включая передачу данных, IP-телефонию, мгновенный обмен сообщениями и присутствие, web-приложения, совместные рабочие пространства, а также аудио- и видеоконференц-связь.

Приведенные далее сценарии демонстрируют примеры осязаемых преимуществ для бизнеса, которые могут быть получены при реализации стратегии на основе политик. Они также иллюстрируют потенциально катастрофические последствия непреднамеренных нарушений безопасности, которые возможны при отсутствии комплексной политики.

Финансовые услуги

В инвестиционно-банковском бизнесе специалисты часто обмениваются с коллегами информацией, которая готовится к включению в полные официальные документы. В этом сценарии сотрудница отдела финансовой аналитики звонит коллеге, чтобы передать черновик отчета по исследованию фармацевтической отрасли для получения его отзывов и проверки достоверности фактов. Она не знает, что коллега уже сменил работу и теперь является брокером в той же фирме, продавая акции фармацевтических предприятий институциональным инвесторам. Жесткий механизм управления политиками в ее организации автоматически

блокирует вызов из-за новой должностной функции ее коллеги. Она пытается связаться с ним по электронной почте и через систему мгновенного обмена сообщениями, но эти каналы также блокируются. Если бы эта политика не применялась, то фирма нарушила бы важнейшее правило Комиссии по ценным бумагам и биржам США в отношении «этических барьеров», что повлекло бы для фирмы значительные штрафы. Это наглядный пример добросовестного сотрудника, потенциально нарушающего крайне серьезную политику без какого-либо злого умысла.

К счастью, прочная структура политик и управления предотвратила этот факт неумышленной передачи сведений и спасла фирму от многомиллионного штрафа.

Нефтегазодобыча

Разведка нефтяных месторождений чрезвычайно дорога и рискованна, поэтому компании часто создают совместные предприятия для распределения затрат на бурение новых скважин. Каждый участник может привнести интеллектуальную собственность: сведения о буровой площадке, методологии бурения и другое техническое ноу-хау. Поскольку сотрудничающие компании одновременно являются конкурентами, то крайне важно, чтобы доступ к ресурсам совместной работы получали только уполномоченные лица, участвующие в совместном предприятии и подписавшие строгие соглашения о конфиденциальности. В отсутствие системы политик управления доступом или полномочиями для работы с конфиденциальными документами и материалами партнерство может не состояться, поскольку отдельные компании, опасаясь за свою конкурентоспособность, скорее всего откажутся от раскрытия значительной доли своего ноу-хау. Однако прочная архитектура на основе политик помогает гарантировать предоставление доступа

к важным данным только лицам с соответствующими должностными функциями и только в рамках соответствующего контекста и условий. Например, система политик может блокировать доступ к ресурсу совместной работы, если пользователь обращается к нему по внешней сети Wi-Fi. При наличии таких контрольных механизмов проект становится осуществимым.

Государственные органы

У федеральных и региональных органов власти может существовать необходимость раскрытия информации только узкому кругу доверенных соотечественников. В этом сценарии правительство США собирает базу данных о террористических угрозах, информацией из которой выборочно обменивается с другими странами. После серии терактов несколько лет назад правительство Индии запросило доступ к базе данных для сравнения информации с донесениями собственной разведки. Ввиду того что информация критически важна для национальной безопасности, правительство США предельно осторожно в вопросах ее передачи третьим сторонам. Но поскольку Индия является союзником, правительство США приняло решение передать отдельные отчеты на фиксированный срок узкому кругу перечисленных лиц в главной спецслужбе Индии. Система управления политиками помогает обеспечить этот предельно ограниченный уровень раскрытия и доступа, регламентируя круг лиц, которым предоставляется доступ к информации, способы ее использования и сроки ее доступности.

Оптимизация совместной работы с практичным управлением политиками

Технологии на основе политик, отмеченные в предыдущих сценариях для сферы финансовых услуг, нефтегазодобычи и государственных органов, уже существуют. Осталось лишь объединить их на комплексной платформе. Стратегическое видение Cisco предполагает применение решения для оптимизации совместной работы, охватывающего все предприятие, включая внутренние и внешние источники данных. Это решение автоматически реализует политики безопасности и управления, открывая возможности для совместной работы между предприятиями с использованием соответствующего коммерческого потенциала всех звеньев – от центра обработки данных до настольного рабочего места.

Для помощи администраторам корпоративных ИТ-систем в обеспечении безопасности сетевых

сред совместной работы компания Cisco разрабатывает свои платформы совместной работы в соответствии с самыми высокими стандартами безопасности и целостности. Далее описаны защищенные решения Cisco® для совместной работы, которые увеличивают практическую эффективность и гибкость различных приложений, устройств, сетей и операционных систем.

Защищенная инфраструктура с Cisco TrustSec и программным обеспечением Cisco IOS

Защищенная инфраструктура – фундаментальный элемент защиты сетевой среды совместной работы. Средства обеспечения высокой доступности (QoS и т. п.) вкупе с динамическим управлением доступом (VLAN и т. п.) делают возможной защищенную совместную работу, в то время как динамическая маркировка устройств и пакетов данных помогает гарантировать применение политики безопасности во всей сети. Эти преимущества не требуют жертвовать существующими инвестициями организации в ИТ и достигаются с применением Cisco TrustSec – новой архитектуры, предусматривающей ряд механизмов масштабируемой защиты коммутаторов.

Защищенное управление доступом в офисном комплексе – единый механизм ролевой идентификации и контролируемого доступа к критически важным приложениям и ресурсам.

Конвергентная система политик – объединение различных ролей, серверов и правил доступа с упрощением управления политиками идентификации.

Повсеместное обеспечение целостности и конфиденциальности данных – защита от утечки данных для соблюдения требований регулирующих органов.

Маршрутизаторы Cisco также предусматривают мощные и адаптируемые решения для безопасности, помогая страховать от атак, провоцирующих отказ в обслуживании (DoS), и других угроз для сетевой инфраструктуры. В состав программного обеспечения Cisco IOS® для маршрутизаторов входит универсальный комплекс технологий безопасности, например межсетевой экран Cisco IOS, система защиты от вторжений (IPS) и средства организации сетей VPN на основе протоколов защиты IPsec и SSL. Эти технологии предлагают следующие преимущества:

- Дополнительная защита без развертывания нового оборудования – реализация новых возможностей безопасности на существующих маршрутизаторах с использованием программного обеспечения Cisco IOS.
- Укрепление безопасности в тех местах, где это более всего необходимо компаниям, – применение функций безопасности (например, межсетевого экрана и системы защиты от вторжений) наряду с централизованным управлением устройствами и политиками в любой точке сети, включая удаленные филиалы.
- Экономия времени и денег – сокращение общего числа устройств в сети с сопутствующим снижением текущих затрат на поддержку и обеспечение управляемости.

Решения Cisco для предотвращения потерь данных

В контексте совместной работы наибольшее беспокойство вызывает рост трафика, пересекающего периметр сети. Решения Cisco для предотвращения потерь данных призваны обеспечить соответствие нормативным требованиям и целостность информации за счет следующих мер.

- Аутентификация пользователей и устройств перед разрешением доступа к сети (посредством технологии Cisco для контроля допуска к сети [NAC]).
- Ведение реестра важных или конфиденциальных сведений, хранящихся на оконечных устройствах, в режиме реального времени и принятие мер для предотвращения непреднамеренной передачи этих сведений неправомочным пользователям или их выгрузки на сменные носители (посредством решения Cisco Security Agent).
- Фильтрация электронной почты для предотвращения распространения конфиденциальной информации по электронной почте (посредством технологии Cisco IronPort®).

Cisco WebEx Connect

Многие аспекты и уровни функций безопасности в Cisco WebEx[®] Connect реализованы в Интересах защиты корпоративных и личных данных, предотвращения несанкционированного доступа и сохранения важных информационных активов бизнеса. Заказчики Cisco WebEx Connect могут рассчитывать на наивысший уровень безопасности за счет применения передовых отраслевых концепций защиты физических объектов, приложений и сети. Cisco WebEx Connect может также использовать Cisco Enterprise Policy Manager – передовое решение по управлению политиками, перешедшее к компании Cisco в результате приобретения фирмы Securent в конце 2007 г.

Представляя собой по-настоящему эффективное решение для совместной работы на основе политик, платформа Cisco WebEx Connect отвечает необходимым требованиям и предлагает развитое ядро политик с поддержкой широкого круга атрибутов, в частности ролей пользователей, ресурсов, времени суток, местоположения в сети, работоспособности устройств, идентификаторов проектов. Решения в политиках могут приниматься на основе сколь угодно большого числа атрибутов. Кроме того, Cisco WebEx Connect предлагает администраторам соответствующего профиля гибкие функции моделирования и делегирования политик, позволяя им тщательно контролировать сеть и доступ к содержимому, задавая политики безопасности с привязкой к бизнес-процессам. В дополнение к этому, Cisco WebEx Connect предусматривает следующие возможности:

- Интеграция с гетерогенными корпоративными решениями для совместной работы и обмена сообщениями без необходимости установки дополнительных решений сторонних производителей, что является важным условием повышения производительности.
- Стабильная производительность и надежность, которые невозможны без многоуровневого подхода и исключения любых критических точек отказа путем полного резервирования всех элементов системы.
- Детализированная регистрация всех событий, включая действия конечных пользователей и операции администраторов, что принципиально важно для обеспечения безопасности и соответствия нормативным требованиям.
- Расширяемая платформа, объединяющая средства мгновенного обмена сообщениями, аудио- видео- и web-конференц-связи, расширяет возможности совместной работы в асинхронном формате и помогает компаниям не отставать от меняющихся производственных потребностей пользователей.

Cisco Enterprise Policy Manager

Для достижения целей, обозначенных в настоящем документе, каждая организация должна развернуть устойчивую корпоративную платформу управления политиками, интегрированную с системой унифицированных коммуникаций и решениями для совместной работы. Cisco Enterprise Policy Manager (EPM) предусматривает развитый набор детализированных функций управления полномочиями для широкого ассортимента корпоративных приложений и хранилищ данных, включая продукты Cisco для унифицированных коммуникаций и Cisco WebEx Connect. Cisco EPM можно использовать для управления политиками, определяющими полномочия пользователей для доступа к документу, просмотра отчетов, выполнения операций, подключения к чату и общения с другими лицами. Вынося политики и управление полномочиями за пределы отдельных приложений, организации получают возможность последовательно применять эти политики в гетерогенной среде приложений с централизованным администрированием и аудитом.

Бесклиентская сеть VPN на основе SSL

Бесклиентская сеть VPN на основе SSL позволяет дистанционным пользователям получать доступ к корпоративным ресурсам практически из любых мест и с любых устройств, например

в дороге или на выставочном стенде. Бесклиентская сеть VPN на основе SSL предусматривает также динамическое ограничение доступа на основе аутентификации пользователя. Эта возможность делает данное решение превосходным вариантом для подрядчиков или гостевых пользователей, которым необходим доступ к сети, которые не могут установить клиент и которым нужно предоставить лишь заранее определенный набор приложений или ресурсов.

Cisco Secure Desktop

Cisco Secure Desktop работает с решением для сети VPN на основе SSL, позволяя создать виртуальную настольную систему на любом оконечном устройстве. Этот продукт позволяет «на лету» преобразовывать многие тысячи приложений с разными форматами интерфейса в формат HTML для работы в web-браузере. Поддерживаются приложения, чувствительные ко времени задержки, благодаря чему работа с приложениями не отличается от работы по локальной сети, несмотря на использование полностью защищенной рабочей среды.

Прокси-сервер для телефонов в устройствах адаптивной защиты Cisco ASA

Прокси-сервер для телефонов в устройствах адаптивной защиты Cisco ASA позволяет сотрудникам, периодически работающим удаленно, подключать IP-телефоны Cisco к своим домашним сетям и использовать встроенные в телефоны средства шифрования для установления защищенных сеансов с корпоративной сетью. Удаленные сотрудники получают возможность работать «как в офисе», имея в своем распоряжении интегрированные коммуникационные инструменты для повышения производительности и налаживания совместной работы. Прокси-сервер для телефонов в составе Cisco ASA может выполнять аутентификацию устройств и оконечную обработку криптографического соединения, связывать телефон с внутренней телефонной сетью, а также шифровать и расшифровывать поток данных между удаленным телефоном, использующим шифрование, и внутренней телефонной сетью без шифрования. Одновременно с перечисленным обеспечиваются необходимые механизмы QoS, выделяющие полосу пропускания для чувствительных к времени задержки сеансов голосовой связи. Кроме того, прокси-сервер для телефонов в Cisco ASA предоставляет удаленным пользователям внутрисетевые службы и рабочие инструменты, не требуя развертывания дополнительных маршрутизаторов или VPN-устройств в домашнем офисе.

Федерация присутствия в Cisco ASA

Федерация присутствия в Cisco ASA создает защищенные сеансы между серверами присутствия Cisco и Microsoft для безопасной совместной работы разных компаний.

Прокси-сервер мобильности Cisco ASA

Прокси-сервер мобильности Cisco ASA позволяет обеспечить защищенное подключение широкого спектра мобильных устройств к внутренней сети.

Cisco Virtual Office

Расширение арсенала инструментов, доступных удаленным работникам, позволяет им активнее взаимодействовать с централизованным штатом. Решение Cisco Virtual Office объединяет продукты, технологии и услуги для предоставления защищенных, информационно насыщенных и управляемых сетевых служб удаленным работникам и сотрудникам, находящимся на удаленных объектах. Решения включают в себя следующие компоненты: средства присутствия для удаленного объекта, средства присутствия для головного узла, набор средств управления и службы для упрощения развертывания и текущего технического обслуживания.

Cisco Virtual Office предлагает пользователям в домашнем или удаленном офисе новый уровень гибкости и производительности со средствами передачи данных, беспроводной связи, голосовой связи, видеосвязи и службами TelePresence «офисного» калибра. Дополняя эти возможности мощными средствами безопасности, компания Cisco предоставляет пользователям гибкость в выборе рабочего графика при работе из дома. Это решение сопровождается моделью

полностью автоматического развертывания, которая существенно повышает эффективность отделов ИТ при экономии времени и затрат. Решение Cisco Virtual Office повышает производительность предприятий, наделяя персонал рабочими инструментами независимо от его местонахождения.

Уверенная совместная работа

Совместная работа предлагает организациям возможность повысить производительность, ускорить внедрение инноваций и обрести конкурентное преимущество. По мере развития организационных структур, способов общения и сетей в геометрической пропорции возрастет актуальность более динамичной и защищенной инфраструктуры для организации совместной работы. С учетом этого компания Cisco наметила основные шаги, которые организации могут предпринять для создания уверенных возможностей совместной работы между внутренними и внешними участниками.

Шаг 1. Определение экосистемы совместной работы.

Для уверенной совместной работы предприятиям необходима экосистема повсеместного взаимодействия, соединяющая рабочие группы на собственной территории с другими участниками в Интернете. Этот шаг помогает улучшить механизмы совместной работы в деловой среде: пользователи по обе стороны межсетевых экранов смогут общаться, не опасаясь за нарушение политики безопасности или нормативных требований. Чтобы сделать первый шаг, организациям необходимо четко определить свои цели в отношении совместной работы, включая рамки поддерживаемых решений и технологий, а также выработать гибкую, ориентированную на перспективу стратегию, оставляющую возможность для совершенствования и роста по мере эволюции потребностей и технологий. Этот подход позволит организациям сохранить конкурентоспособность, избегая необходимости замены дорогостоящих устройств или решений, которые оказываются неспособны удовлетворить перспективные требования безопасности и совместной работы.

Шаг 2. Выработка политик.

Следующий шаг – определение концепции безграничного предприятия с регулирующими политиками, где все получают возможность уверенно сотрудничать и совместно использовать информацию в актуальном контексте, ускоряя тем самым новаторство в бизнесе. Сеть в этой среде станет основой для защищенных доверенных сообществ через тесное взаимодействие между фундаментальными механизмами сетевой безопасности и устройствами защиты с поддержкой совместной работы. Такой подход опирается на повсеместное развертывание корпоративных политик, предусматривающих динамическое персонализированное определение действий одновременно с реализацией нормативных требований. Для того чтобы развертывание средств совместной работы в этой безграничной среде имело наибольший эффект, политики должны быть интегрированы в укрупненные политики корпоративной безопасности и сетевые политики. Это помогает гарантировать, что существующие политики не станут излишне ограничивать возможности развертывания новых решений для совместной работы, и наоборот, что эти новые инструменты совместной работы не создадут для предприятия новых рисков, не покрываемых фундаментальными политиками в области безопасности и сетей.

Шаг 3. Создание культуры совместной работы.

Изменение природы предприятий привело к увеличению численности удаленных сотрудников, удаленных офисов и выездных сотрудников. Увеличение и рассредоточение штата диктуют необходимость постоянной доступности сетевых служб и ресурсов хранения данных всюду, где в них может возникнуть потребность. Совместная работа в этой среде будет иметь место и дома, и в дороге, что потребует интеграции интеллектуальных средств безопасности удаленных подключений и сети

наряду с расширением арсенала сетевых служб и средств совместной работы. Такой интегрированный подход позволит организовать доступ, регламентируемый политиками, и глубокий анализ трафика независимо от местонахождения инициатора связи, а также применяемых устройств и методов доступа.

В число главных технологий, на которых базируется это стратегическое видение, входят распределение ресурсов и управление ими. Эта технология помогает гарантировать, что сеть будет в состоянии предложить насыщенный формат совместной работы соответствующим пользователям, не потребляя всю доступную полосу пропускания. В среде, поддерживающей культуру совместной работы, решения на основе политик будут выполнять сторожевую функцию, изменяя поведение пользователей без необоснованных отказов в доступе.

Заключение

Унифицированные коммуникации и ставшие возможными благодаря им механизмы совместной работы – это больше чем инструменты повышения эффективности. Это стратегия, представляющая первоочередную важность для руководителей предприятий. Организации, которые смогут наиболее эффективно внедрить и использовать эти технологии, получают более высокую динамичность и возможность дифференцировать себя в сегодняшних условиях конкуренции.

Лучшие решения, позволяющие достичь такого уровня защищенной совместной работы, требуют всесторонней архитектуры на основе политик, которая динамически профилирует действия пользователей и предусматривает детальное управление доступом на уровне сети. Этот подход решает вопросы соответствия нормативным требованиям и позволяет как пользователям, так и компаниям уверенно сотрудничать всегда, везде, с любыми партнерами и на любых устройствах.

Специалисты компании Cisco хорошо представляют себе потребности сотрудников, работающих совместно как в офисах компаний, так и удаленно, а также пользователей аутсорсинговых платформ, размещенных в сети. Cisco стремится предложить общую платформу, обеспечивающую надлежащий уровень безопасности и механизмы QoS для каждой конкретной формы взаимодействия. Открывая путь к созданию защищенных, ориентированных на совместную работу сред, компания Cisco по-настоящему ускоряет работу бизнеса и позволяет организациям свободно обмениваться данными, побуждать, изобретать, сотрудничать и вести деятельность без рисков, уверенно работая в совместном формате.



Cisco Россия, 115054, Москва, бизнес-центр «Риверсайд Тауерс» Космодамианская наб., 52, стр. 1, этаж 4 Тел.: +7 (495) 961 14 10 Факс: +7 (495) 961 14 60 www.cisco.ru www.cisco.com	Cisco Россия, 191186, Санкт-Петербург, бизнес-центр «Регус» Невский проспект, 25, этаж 2, офис 30 Тел.: +7 (812) 346 77 17 Факс: +7 (812) 346 78 00 www.cisco.ru www.cisco.com	Cisco Казахстан, 480099, Алматы, бизнес-центр «Самал 2» Ул. О. Жолдасбекова, 97, блок А2, этаж 14 Тел.: +7 (727) 244 21 01 Факс: +7 (727) 244 21 02 www.cisco.ru www.cisco.com	Cisco Украина, 03038, Киев, бизнес-центр «Горизонт Парк» (Horizon Park) Ул. Николая Гринченко, 4В Тел.: +7 (38044) 391 36 00 Факс: +7 (38044) 391 36 00 www.cisco.ua www.cisco.com	Cisco Азербайджан, AZ 1065, Баку, бизнес-центр «Карат» Ул. М. Мухтарова, 201, этаж 2 Тел.: +7 (99412) 437 48 20 Факс: +7 (99412) 437 48 21 www.cisco.ru www.cisco.com	Cisco Узбекистан, 100000, Ташкент, бизнес-центр «ИНКОНЕЛЬ» Ул. Пушкина, 75, офис 605, этаж 6 Тел.: +7 (99871) 140 44 60 Факс: +7 (99871) 133 44 64 www.cisco.ru www.cisco.com
---	--	--	--	---	---

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the [Cisco Website at www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2007 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

© Cisco Systems, Inc., 2007 г. Все права защищены. Данный документ относится к публичной информации Cisco.