



Защищенный мобильный клиент Cisco AnyConnect Secure Mobility

Предоставьте вашим сотрудникам возможность работать в любой точке света — не только на корпоративных ноутбуках, но и на личных мобильных устройствах. Обеспечьте необходимый уровень информационной безопасности данных вашей организации. Вот что включает в себя защищенный мобильный клиент Cisco AnyConnect® Secure Mobility (рис. 1). Cisco AnyConnect — это единый агент, предоставляющий ряд услуг обеспечения безопасности для защиты предприятия. Он обеспечивает необходимый уровень контроля, позволяя определить, какие пользователи и программы получают доступ к системам предприятия до, во время и после атаки. Защищенный мобильный клиент AnyConnect® Secure Mobility предоставляет комплексную платформу обеспечения (сетевой) безопасности оконечных устройств с функциями удаленного доступа, применения политик и обеспечения безопасности интернет-трафика. AnyConnect предоставляет ИТ-подразделению все необходимые функции безопасного доступа для надежной, комфортной и совершенно безопасной работы на мобильных устройствах.

Преимущества

Для конечных пользователей

- Высокозащищенная мобильность на распространенной платформе для мобильных устройств
- Унифицированная рабочая среда для пользователей
- Интеллектуальное, надежное и постоянное подключение

Для администраторов информационной безопасности

- Увеличенная производительность и низкая совокупная стоимость владения в одном клиенте
- Комплексный и удобный мониторинг соблюдения политик безопасного доступа с учетом контекста
- Гибкий доступ к корпоративным ресурсам и приложениям на основе правил для каждой группы пользователей и устройства через проводные и беспроводные сети, а также VPN

Рис. 1. Клиент AnyConnect Secure Mobility



Функциональные возможности и преимущества

Защищенный мобильный клиент AnyConnect Secure Mobility — это лучший в отрасли многофункциональный программный продукт для оконечных устройств. Он не только предоставляет VPN-доступ по протоколам SSL и IPsec IKEv2, но и обеспечивает повышенную информационную безопасность с помощью различных встроенных модулей. Эти модули позволяют пользоваться множеством функциональных услуг, включая обеспечение соответствия нормативным требованиям с помощью политик VPN и платформы Cisco Identity Services Engine (ISE), безопасности интернет-трафика, контроль состояния сети и диспетчера сетевого доступа. Клиент AnyConnect совместим с целым рядом платформ, включая Windows, ОС Mac X, Linux, IOS, Android, Windows Phone, BlackBerry и Google Chrome (ранняя предварительная версия).

Дальнейшие шаги

Для получения дополнительной информации посетите следующие сайты:

- Лицензирование и оформление заказа: в [руководстве по оформлению заказа на Cisco AnyConnect](#) приведена информация о лицензировании для AnyConnect, SSL VPN без клиентской программы и использовании VPN для удаленного доступа по протоколу IKEv2.
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility: <http://www.cisco.com/go/anyconnect>.
- Многофункциональное устройство защиты Cisco ASA серии 5500-X: <http://www.cisco.com/go/asa>.

Основные возможности указаны в таблице 1.

Таблица 1. Возможности защищенного мобильного клиента AnyConnect Secure Mobility

Функц. возможность	Описание
Единая система соответствия оконечных устройств нормативным требованиям	Агент AnyConnect ISE обеспечивает универсальное применение политик и восстановление для платформы Cisco ISE в средах на базе проводных, беспроводных сетей и VPN-решений. Услуги как основной источник применения политик оконечных устройств с проверкой версий ОС и последних антивирусных обновлений, а также другими ресурсами для повышения информационной безопасности оконечных устройств и их соответствия нормативным требованиям. Кроме того, получить доступ к политикам оконечных устройств в Cisco Hostscan можно с помощью адаптивного устройства обеспечения безопасности.
Защищенный сетевой доступ	Диспетчер сетевого доступа AnyConnect располагает широчайшими возможностями подключения. Администраторы могут определять, к каким сетям или ресурсам могут подключаться оконечные устройства. Он предоставляет запрашивающее устройство IEEE 802.1X, которое может быть выделено как часть функций аутентификации, авторизации и учета (AAA) наряду с некоторыми уникальными технологиями шифрования, такими как MACsec IEEE 802.1AE.
Обеспечение безопасности веб-трафика	В Cisco AnyConnect встроен модуль, реализующий обеспечение безопасности веб-трафика с помощью локальных устройств обеспечения безопасности веб-трафика Cisco или облачной системы защиты веб-трафика Cisco Cloud Web Security. Сочетая средства обеспечения безопасности интернет-трафика с VPN-доступом, администраторы могут гарантировать комплексную защиту мобильности для всех конечных пользователей, что крайне важно для сред, построенных по принципу «Принеси на работу свое устройство» (Bring Your Own Device, BYOD). Предприятия могут выбрать нужный вариант развертывания для защиты сети от вредоносного веб-ПО и контроля использования Интернета.
Мониторинг сети	Модуль контроля состояния сети AnyConnect на платформах Windows и Mac OS X позволяет администраторам отслеживать использование приложений на оконечных устройствах, что дает возможность выявлять потенциальные отклонения в поведении и принимать более рациональные решения при проектировании сетей. Данные об использовании можно параллельно использовать в многочисленных средствах анализа сети с поддержкой протокола IPFIX.
Доступ без клиентской программы	Многофункциональные устройства обеспечения безопасности Cisco ASA поддерживают подключение по протоколу SSL через множество браузеров для самых разных платформ. Администраторы могут предоставлять VPN-доступ к неуправляемым терминальным устройствам без клиентской программы. Также поддерживается доступ к различным веб- и TCP/IP-приложениям. Доступ осуществляется через модуль переопределения, подключаемые модули или интеллектуальные туннели с помощью встроенной браузерной SSL-технологии. При этом гарантируется тщательное управление доступом и комплексная информационная безопасность.
Доступ к инфраструктуре виртуальных настольных систем (VDI)	Многофункциональные устройства защиты Cisco ASA могут прерывать сеанс VDI с высоким уровнем информационной безопасности, а также обеспечивать прозрачный доступ к виртуализированным приложениям и рабочим столам. Для мобильных устройств, ноутбуков и настольных устройств предлагается доступ к виртуальным ресурсам как с клиентской программой, так и без нее. Доступ к виртуальным ресурсам на базе защищенного удаленного доступа независим от поставщика и подчиняется единой политике доступа, определенной для виртуальных и традиционных ресурсов.
Поддержка мобильных устройств	В связи с распространением концепции BYOD администраторы вынуждены поддерживать работу конечных пользователей, предоставляя их личным мобильным устройствам удаленный доступ к корпоративным сетям. AnyConnect можно развернуть на самых распространенных устройствах, используемых современными сотрудниками. Надежно защищенный удаленный доступ может быть основан на устройствах или предоставляться прозрачным образом определенными корпоративными мобильными приложениями с отдельными VPN. Новая функция с отдельными VPN для каждого приложения исключает несанкционированный доступ приложений к конфиденциальным бизнес-ресурсам, значительно сокращая риск вторжения вредоносного ПО и затраты на пропускную способность для удаленного доступа.