Защищенный мобильный клиент Cisco AnyConnect Secure Mobility для мобильных платформ

Защищенный мобильный клиент Cisco AnyConnect® Secure Mobility для мобильных платформ обеспечивает надежные и удобные в развертывании зашифрованные сетевые подключения со смартфонов и планшетов, а также постоянный корпоративный доступ для мобильных сотрудников.

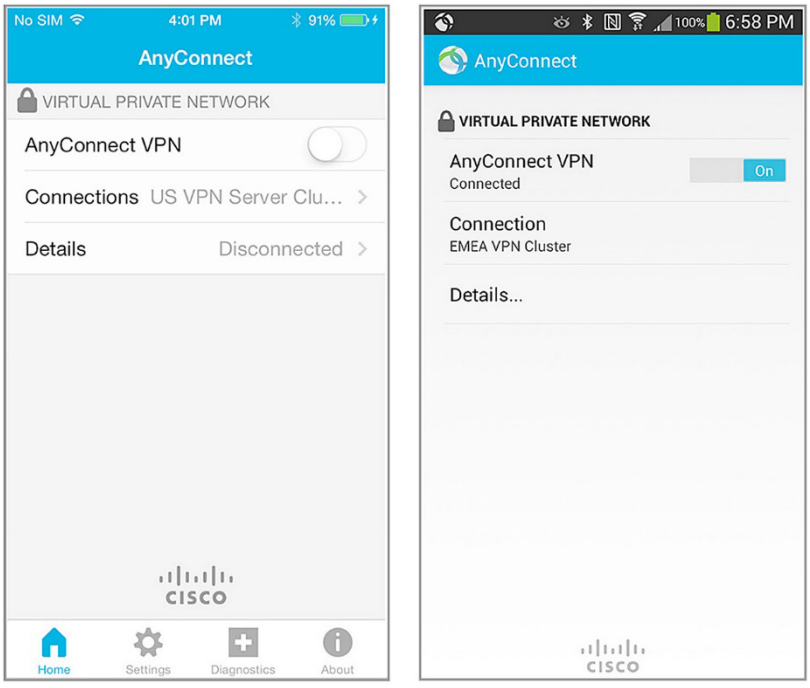
Обзор продукта

Теперь появилась возможность обезопасить смартфоны и планшеты сотрудников с помощью защищенного мобильного клиента Cisco AnyConnect Secure Mobility для мобильных платформ, доступного для Apple iOS, Android, Windows Phone 8.1, BlackBerry 10.3.2 и более поздних версий, некоторых устройств Amazon Kindle и Fire Phone, а также Google Chrome OS (ранняя предварительная версия).

Неважно, открывают ли сотрудники свою деловую электронную почту, сеанс связи с виртуальной настольной системой или другие корпоративные приложения, клиент AnyConnect предоставит им удобный в работе интерфейс для критически важной информации. Клиент использует протоколы Datagram Transport Layer Security (DTLS), IPsec IKEv2 и TLS (HTTP через TLS/SSL) для предоставления важных для бизнеса приложений, включая приложения, требующие минимальных задержек, такие как VoIP, с зашифрованным доступом к корпоративным ресурсам. AnyConnect 4.x поддерживает функции VPN для отдельных приложений для iOS 8.3 и более поздних версий.

На рис. 1 показан пример интерфейса пользователя AnyConnect на устройствах Apple iOS и Android.

Рисунок 1. Интерфейс пользователя на устройствах Apple iOS и Android



Функциональные возможности и преимущества

В таблице 1 приведены возможности и преимущества защищенного мобильного клиента Cisco AnyConnect Secure Mobility для мобильных платформ. Доступность функций зависит от платформы. Подробные сведения о поддерживаемых функциях для конкретных операционных систем вы можете найти в примечаниях к выпускам платформ и документации.

Таблица 1. Функциональные возможности и преимущества

Функц. возможность	Преимущество
Доступ и совместимость программного обеспечения	**Доступно на порталах приложений** • **Магазин приложений Apple:** для Apple iOS 6.0 и более поздних версий • **Google Play:** для Android 4.0 и более поздних версий Обратите внимание, что доступно несколько образов AnyConnect, поэтому важно правильно выбрать подходящий вариант для своего устройства. Конкретные требования вы можете найти в примечаниях к выпускам Android. • **Windows Store:** для Windows Phone 8.1 Update 1 и более поздних версий • **BlackBerry App World:** для BlackBerry 10.3.2 и более поздних версий • **Google Chrome OS:** для Chrome OS 43 и более поздних версий (ранняя предварительная версия) • **Amazon Appstore:** для некоторых устройств Kindle и Fire Phone
Оптимизированный сетевой доступ	• Автоматически адаптирует протокол туннелирования под самый эффективный метод в соответствии с ограничениями сети. • Использует протокол DTLS для предоставления оптимизированного подключения для доступа к приложениям на основе TCP и трафика, требующего минимальных задержек, например трафика VoIP. • Использует протокол TLS (HTTP через TLS/SSL) для обеспечения доступности сетевых подключений в заблокированных средах. • IPsec IKEv2 обеспечивает оптимизированное подключение для чувствительного к задержкам трафика в случае, если политики безопасности требуют использования протокола IPsec (требуется многофункциональное устройство обеспечения безопасности Cisco ASA 8.4 или более поздней версии) • Совместим с функций распределения нагрузки ASA VPN
Удобство мобильного доступа	• Восстанавливает работу прозрачным способом после изменения IP-адреса, потери подключения или вывода устройства из режима ожидания
Оптимизированное энергопотребление	• Учитывает особенности режима ожидания устройства
Шифрование	• Поддержка криптостойкого шифрования, включая AES-256 и 3DES-168. (Шлюз информационной безопасности должен иметь активированную лицензию на криптостойкое шифрование.) • Шифрование нового поколения, включая алгоритмы NSA Suite B, ESPv3 с IKEv2, 4096-разрядные ключи RSA, протокол Diffie-Hellman group 24 и расширенный функционал SHA2 (SHA-256 и SHA-384). Доступен только для подключений IPsec IKEv2. Требуется лицензия AnyConnect Apex.
Варианты проверки подлинности	• RADIUS • RADIUS с истечением срока действия пароля (MSCHAPv2) и NT LAN Manager (NTLM) • RADIUS с поддержкой одноразовых паролей (OTP) (атрибуты ответного сообщения и состояния) • Метки RSA SecurID • Active Directory или Kerberos • Цифровой сертификат (совместим со встроенным протоколом SCEP AnyConnect для развертывания учетных данных) • Стандартная поддержка протокола LDAP • Протокол LDAP с истечением срока действия пароля и отслеживанием устаревания пароля • Объединенная многофакторная проверка подлинности на основе сертификата и имени пользователя или пароля (двойная проверка подлинности)
Унифицированная рабочая среда для пользователей	• Режим полного туннелирования клиента поддерживает удаленных пользователей, которым необходима унифицированная рабочая среда, аналогичная той, которой они пользуются в локальной сети
Централизованное управление и контроль политик	• Политики можно предварительно конфигурировать или конфигурировать локально, а также автоматически обновлять со шлюза безопасности VPN • Обработчик универсальных кодов ресурсов (URI) для AnyConnect позволяет легко проводить развертывания с помощью URL-адресов, встроенных в веб-страницы или приложения. • Сертификаты можно просматривать и управлять ими локально

Функц. возможность	Преимущество
Расширенные возможности подключения по IP-сети	• Политика сетевого доступа с раздельным и полным туннелированием под управлением администратора • Политика VPN-подключения для каждого приложения для iOS 8.3 и более поздних версий (требуется многофункциональное устройство защиты Cisco ASA 5500-X с OS 9.3.2 или более поздней версии и лицензиями AnyConnect Plus или Apex) • Политика управления доступом **Способы назначения IP-адреса:** • Статическая настройка • Внутренний пул • Протокол динамической конфигурации узла сети (DHCP) • RADIUS/LDAP
Локализация	**Помимо английского языка клиент переведен на следующие языки:** • Канадский французский (fr-ca) • Чешский (cs-cz) • Немецкий (de-de) • Японский (ja-jp) • Корейский (ko-kr) • Испанский, Латинская Америка (es-co) • Польский (pl-pl) • Упрощенный китайский (zh-cn)
Диагностика	• Доступны встроенные возможности сбора информации о входе и статистики. • Журналы можно просматривать на устройстве. • Журналы можно легко отправить по электронной почте в Cisco или администратору для анализа.

Совместимость с платформами

Защищенный мобильный клиент AnyConnect Secure Mobility совместим со всеми моделями серийных межсетевых экранов нового поколения Cisco ASA серии 5500-X и Cisco серии 5500 Enterprise Firewall Edition под управлением программного обеспечения ASA версии 8.0(4) или более поздних версий. Рекомендуется использовать текущие выпуски программного обеспечения ASA.

Для некоторых функций требуются более поздние выпуски программного обеспечения ASA или модели ASA 5500-X.

Cisco поддерживает VPN-доступ AnyConnect к ОС Cisco IOS® версии 15.1(2)T или более поздних версий, функционирующим в качестве надежно защищенного шлюза с определенными ограничениями функционала. Более подробную информацию см. в разделе Функции, не поддерживаемые Cisco IOS SSL VPN. Дополнительную информацию о поддержке функций ПО Cisco IOS см. по адресу http://www.cisco.com/go/fn.

Дополнительную информацию о совместимости см. по адресу http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Информация о вариантах лицензирования и оформлении заказа

В руководстве по оформлению заказа на AnyConnect приведена информация о лицензировании и оформлении заказа для использования AnyConnect, SSL VPN без клиентской программы и VPN сторонних производителей для удаленного доступа по протоколу IKEv2. Для полной поддержки платформ и функций требуются лицензии AnyConnect Plus или Apex. Заказчики с действующими лицензиями Essentials или Premium и мобильными лицензиями могут пользоваться версиями для iOS и Android (за исключением функций VPN для отдельных приложений) до 30 апреля 2016 года. Для всех других мобильных платформ требуются лицензии Plus или Apex. Подключение AnyConnect VPN к оборудованию головных станций сторонних производителей не допускается. Дополнительную информацию можно найти в руководстве по оформлению заказа по адресу http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

Cisco Capital

Возможности финансирования, которые помогут в достижении поставленных целей

Программы финансирования Cisco Capital помогут вам приобрести технологии, необходимые для достижения поставленных целей и обеспечения конкурентоспособности. Мы поможем вам снизить капитальные затраты. Ускорить развитие бизнеса. Оптимизировать инвестиции и их окупаемость. Программы финансирования Cisco Capital обеспечивают гибкие возможности при приобретении оборудования, программного обеспечения, сервисов и дополнительного оборудования сторонних производителей. И это всего лишь за один прогнозируемый платеж. Программами Cisco Capital можно воспользоваться более чем в 100 странах. Подробнее.

Дополнительная информация

- Домашняя страница клиента Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect.
- Документация Cisco AnyConnect: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.
- Серийные межсетевые экраны нового поколения Cisco ASA серии 5500-X: http://www.cisco.com/go/asa.
- Лицензионное соглашение и политика конфиденциальности Cisco AnyConnect: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html.

Благодарности

Этот продукт содержит программное обеспечение, разработанное группой OpenSSL Project для использования в наборе инструментальных средств OpenSSL Toolkit.

Этот продукт содержит криптографическое программное обеспечение, написанное Эриком Янгом (Eric Young).

Этот продукт содержит криптографическое программное обеспечение, написанное Тимом Хадсоном (Tim Hudson).

Этот продукт включает HTTP-библиотеку libcurl: авторские права Copyright 1996–2006, Дэниэл Штенберг (Daniel Stenberg).

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Напечатано в США

C78-527494-09, октябрь 2015 г.