Защищенный мобильный клиент Cisco AnyConnect Secure Mobility Client

Удобство использования. Высокий уровень безопасности. Эти достоинства делают клиент для безопасного доступа с мобильных устройств Cisco AnyConnect® Secure Mobility Client одним из самых популярных в мире. Заказчики уже знают, что каждая новая версия AnyConnect® — это новый высочайший уровень технологии удаленного доступа для широкого спектра мобильных устройств и ПК.

Обзор продукта

Мобильные сотрудники часто перемещаются с места на место, но всегда подключенная интеллектуальная VPN-сеть позволяет клиентским устройствам автоматически выбирать оптимальную точку доступа к сети и адаптирует протокол туннелирования, выбирая наиболее эффективный способ. Например, это может быть протокол Datagram Transport Layer Security (DTLS) для чувствительного к задержкам трафика, передачи голоса по IP (трафик VoIP) или доступа к приложениям на основе TCP. Поддержка туннелирования также доступна для IP Security Internet Key Exchange версии 2 (IPsec IKEv2). Выбор доступа к приложениям через VPN можно включить на устройствах Apple iOS, Google Android (версии 5.0 и более поздних) и Samsung KNOX с функцией VPN доступа для каждого приложения в версии 4.x.

AnyConnect 4.x поддерживает надежные функции соответствия оконечных устройств унифицированным политикам. Решение обеспечивает целостность корпоративной сети за счет ограничения доступа по VPN на многофункциональном устройстве обеспечения безопасности Cisco ASA на основе оценки состояния безопасности оконечного устройства. Функция оценки состояния оконечного устройства и его восстановления в проводных и беспроводных средах обеспечивает проверку статуса различного антивирусного ПО, персональных межсетевых экранов или решений для обнаружения шпионских программ. В случае если оконечное устройство не удовлетворяет требованиям безопасности, предлагаются варианты для восстановления и проводятся дополнительные системные проверки, прежде чем будет предоставлен доступ.

Решение AnyConnect Secure Mobility включает встроенные функции обеспечения безопасности веб-трафика, защиты от вредоносного ПО, защиту от фишинга, блокирование обратного вызова команд и средств управления, а также удаленный доступ для создания комплексного и высоко безопасного корпоративного мобильного решения. Для обеспечения безопасности веб-трафика и надежного, высокозащищенного доступа сотрудников к корпоративным ресурсам предлагается аппаратная или облачная версия устройства для защиты веб-трафика — Cisco Web Security Appliance или Cisco Cloud Web Security соответственно. Для защиты в случае, когда VPN-доступ отключен, предлагается облачный сервис безопасности Cisco Umbrella Roaming, который позволяет защитить устройства от вредоносного ПО, фишинга и обратного вызова команд и средств управления в любом месте.

С помощью модуля Сетевого мониторинга на платформах Windows и Mac OS X администраторы могут контролировать использование приложений на оконечных устройствах на предмет выявления потенциальных аномалий в поведении и принятия более обоснованных решений в плане дизайна сети. Данные об использовании приложений можно передавать в самые разные инструменты сетевого анализа с поддержкой Internet Protocol Flow Information Export (IPFIX), например, Cisco StealthWatch.

С появлением решения Cisco Advanced Malware Protection (AMP) Enabler, AnyConnect теперь можно использовать для развертывания решения Cisco Advanced Malware Protection для оконечных устройств. Такая возможность значительно расширяет функционал защиты от угроз для оконечных устройств с VPN-подключением, а также любых используемых сервисов AnyConnect (для доступа к сети 802.1X, оценки состояния и т. д.). Кроме того, значительно снижается риск атак с узлов, подключенных к предприятию. Лицензия на AMP для оконечных устройств приобретается отдельно от лицензии на AnyConnect.

Помимо лучших в отрасли возможностей VPN мобильный клиент AnyConnect поддерживает возможности IEEE 802.1X, обеспечивая единую структуру аутентификации для управления идентификацией пользователей и устройств наряду с протоколами сетевого доступа, необходимыми для беспроблемного перехода от проводных к беспроводным

сетям.

Так как функциональность VPN полностью согласована с клиентом, клиент поддерживает стандарт IEEE 802.1AE Media Access Control security (MACsec) для обеспечения конфиденциальности и целостности данных и аутентификации происхождения данных в проводных сетях, обеспечивая защиту коммуникаций между доверенными компонентами в сети.

На рис. 1 представлен пример конфигурации VPN на ОС Microsoft Windows.

Рисунок 1. Значок и пример конфигурации VPN в Microsoft Windows

На рис. 2 представлен пример конфигурации VPN на Apple OS X.

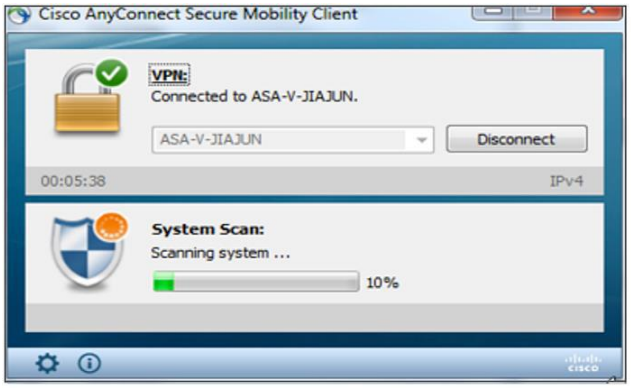
Рисунок 2. Значок и пример конфигурации VPN на Apple OS X

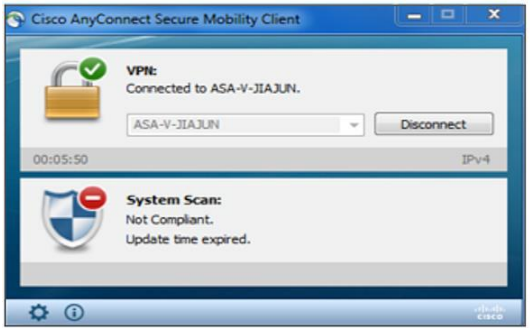
Модули клиента

AnyConnect — это облегченный клиент безопасности с модульной структурой, предоставляющий удобные возможности, настраиваемые пользователем с учетом индивидуальных бизнес-потребностей. Такие функции, как VPN, 802.1X, проверка соответствия политикам, сетевой мониторинг, Cisco Umbrella Roaming, интеграция с облачным устройством защиты веб-трафика Cisco Cloud Web Security, а также возможность установки или удаления решения AMP для оконечных устройств, реализованы в качестве отдельно развертываемых модулей или сервисов, что позволяет организациям выбирать функции и функциональность, наиболее соответствующие их потребностям в сетевом подключении. Такой подход обеспечивает гибкость и операционную эффективность клиента AnyConnect, одновременно предоставляя преимущества и оперативность для организации.

На рис. 3 представлен процесс проверки соответствия оконечных устройств унифицированным политикам в проводных и беспроводных средах.

Рисунок 3. Проверки соответствия оконечных устройств политикам безопасности





Функции и преимущества

В таблице 1 приведены возможности и преимущества клиента Cisco AnyConnect Secure Mobility.

Таблица 1. Функции и преимущества

Функция	Преимущества и описание
Удаленный VPN-доступ	
Поддержка широкого спектра операционных систем	• Windows 10, 8.1, 8 и 7 • Mac OS X 10.8 или выше • Linux Intel (x64) • Информацию о мобильной платформе см. в Информационном бюллетене AnyConnect Mobile
Доступ к программному обеспечению	• Программное обеспечение можно загрузить в Центре поддержки ПО на сайте Cisco.com. • Возможность использования технической поддержки и программного обеспечения для AnyConnect включена во все лицензии Plus и Apex с ограниченным сроком действия, а для бессрочных лицензий Plus может быть приобретена отдельно. • Номер договора должен быть связан с идентификатором на сайте Cisco.com ID. Более подробную информацию см. в Руководстве по заказу решения AnyConnect.
Оптимизированный доступ к сети: выбор VPN-протокола SSL (TLS и DTLS); IPsec IKEv2.	• AnyConnect позволяет выбирать VPN-протоколы, что дает возможность администраторам использовать те протоколы, которые наиболее подходят для выполнения бизнес-задач. • Поддержка туннелирования включает SSL (TLS 1.2 и DTLS) и IPsec (Internet Key Exchange версии 2) KEv2 нового поколения. • DTLS обеспечивает оптимизированное подключение для чувствительного к задержкам трафика, например, трафика VoIP или доступа к приложениям на основе TCP. • TLS 1.2 (HTTP через TLS или SSL) помогает обеспечить доступность сетевых подключений в защищенных средах, включая среды с использованием серверов веб-прокси. • IPsec IKEv2 обеспечивает оптимизированное подключение для чувствительного к задержкам трафика в случае, когда политики безопасности требуют использование протокола IPsec.
Оптимальный выбор шлюза	• Определяет и устанавливает соединение с оптимальной точкой доступа к сети, поэтому конечным пользователям не нужно самостоятельно определять ближайшее местоположение точки доступа.
Удобство мобильного доступа	• Предназначен специально для мобильных пользователей. • Можно сконфигурировать таким образом, чтобы VPN-подключение продолжало работать даже при изменении IP-адреса, прерывании соединения, в спящем режиме или в режиме ожидания.

Функция	Преимущества и описание
	• Благодаря функции обнаружения доверенных сетей Trusted Network Detection VPN-подключение может автоматически отключаться, когда пользователь находится в офисе, и снова подключаться, когда пользователь находится в удаленном местоположении.
Шифрование	• Поддержка криптостойкого шифрования, включая AES-256 и 3DES-168. (Шлюз 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). Применяется только для подключений IPsec IKEv2. Необходима лицензия AnyConnect Apex.
Широкий выбор вариантов развертывания и подключения	**Варианты развертывания** • Предварительное развертывание, включая Microsoft Installer. • Автоматическое развертывание шлюза безопасности (для первоначальной установки необходимы права администратора) с использованием ActiveX (только для Windows) и Java. **Режимы подключения** • Значок автономной системы. • Запуск через браузер (через Интернет). • Активация портала без использования клиента. • Активация через интерфейс командной строки. • Активация через API-интерфейс.
Широкий выбор вариантов подключения	• RADIUS. • RADIUS с истечением срока действия пароля (MSCHAPv2) и NT LAN Manager (NTLM). • RADIUS с поддержкой одноразовых паролей (OTP) (атрибуты ответного сообщения и состояния). • RSA SecurID (включая интеграцию SoftID). • Active Directory или Kerberos. • Встроенный центр сертификации (CA). • Цифровой сертификат или смарт-карта (включая поддержку сертификата компьютера), устанавливается автоматически или выбирается пользователем. • Протокол Lightweight Directory Access Protocol (LDAP) с истечением срока действия пароля и отслеживанием устаревания пароля. • Общая поддержка LDAP. • Объединенная многофакторная аутентификация на основе сертификата и имени пользователя или пароля (двойная аутентификация).
Унифицированная рабочая среда для пользователей	• Режим полного туннелирования клиента поддерживает удаленных пользователей, которым необходима унифицированная рабочая среда, аналогичная их среде в локальной сети. • Различные способы доступа к приложениям обеспечивают широкую совместимость клиента AnyConnect. • Пользователь может отложить установку обновлений. • Возможность получения обратной связи от заказчика.
Централизованное управление и контроль политик	• Политики можно предварительно конфигурировать или конфигурировать локально, а также автоматически обновлять со шлюза безопасности VPN. • API-интерфейс для AnyConnect облегчает развертывание с использованием веб-страниц или приложений. • Проверка и предупреждения пользователей о ненадежных сертификатах. • Сертификаты можно просматривать и управлять ими локально.
Расширенные возможности подключения по IP-сети	• Общедоступные подключения к сетям и с сетей IPv4 и IPv6. • Доступ к внутренним сетевым ресурсам IPv4 и IPv6. • Политика доступа к сети с раздельным и полным туннелированием под управлением администратора. • Политика управления доступом. • Политика VPN-подключения для каждого приложения для Google Android (Lollipop) и Samsung KNOX (новое в версии 4.0: необходимо устройство Cisco ASA 5500-X с OS 9.3 или более поздней версии и лицензиями AnyConnect 4.0). **Способы назначения IP-адреса** • Статическая настройка. • Внутренний пул. • Протокол динамической конфигурации узла сети (DHCP). • RADIUS/упрощенный протокол доступа к каталогам (LDAP).
Полное соответствие оконечных устройств унифицированным политикам (необходима лицензия Apex).	• Оценка состояния оконечных устройств и их восстановление для проводных и беспроводных сред (вместо агента Cisco Identity Services Engine NAC Agent). Требуется Identity Services Engine 1.3 или более поздней версии с лицензий Cisco Identity Services Engine Apex. • Прежде чем предоставить доступ к сети, функции оценки состояния ISE Posture (работая вместе с ISE) и Hostscan (только VPN) проверяют оконечное устройство на наличие антивирусного ПО, пакетов обновления/исправления Windows и ряда других программных сервисов. • Администраторы также имеют возможность проводить пользовательские проверки состояния на предмет наличия выполняемых процессов. • ISE Posture и Hostscan могут устанавливать наличие водяного знака на удаленной системе. Водяной знак может использоваться для идентификации активов, принадлежащих предприятию, и предоставлять дифференцированный доступ на основе этой информации. Проверка водяных знаков включает проверку значения реестра системы, наличия файла, соответствующего требуемой контрольной сумме CRC32, соответствия диапазону IP-адресов и ряда других возможностей. Для приложений, не соответствующих требованиям политик, предусмотрены дополнительные возможности. • Функции зависят от операционной системы. Более подробную информацию см. в диаграммах Host Scan.
Политика межсетевого экрана	• Обеспечивает дополнительную защиту для конфигураций раздельного туннелирования.

Функция	Преимущества и описание
клиента	• Используется вместе с клиентом AnyConnect, чтобы разрешить исключения для локального доступа (например, печать на принтере, поддержка связанного устройства и т. д.). • Поддерживает правила на основе портов для IPv4 и сети и списки контроля IP-доступа (ACLs) для IPv6. • Доступно для платформ Windows и Mac OS X.
Локализация	**Помимо английского языка клиент переведен на следующие языки:** • Чешский (cs-cz) • Немецкий (de-de) • Испанский (es-es) • Французский (fr-fr) • Японский (ja-jp) • Корейский (ko-kr) • Польский (pl-pl) • Упрощенный китайский (zh-cn) • Китайский (Тайвань) (zh-tw) • Голландский (nl-nl) • Венгерский (hu-hu) • Итальянский (it-it) • Португальский (Бразилия) (pt-br) • Русский (ru-ru)
Удобное администрирование клиента	• Администраторы могут автоматически распределять обновления программного обеспечения и политик с головного устройства безопасности, таким образом устраняя необходимость выполнять операции администрирования, связанные с обновлением ПО клиента. • Администраторы могут задавать, какие возможности сделать доступными в конфигурации для конечного пользователя. • Администраторы могут инициировать сценарий оконечного устройства при подключении и отключении, если нельзя использовать сценарии входа для домена. • Администраторы могут полностью настроить и локализовать сообщения для конечного пользователя.
Редактор профилей	• Политики AnyConnect можно настраивать непосредственно с диспетчера Cisco Adaptive Security Device Manager (ASDM).
Диагностика	• 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.
Федеральный стандарт по обработке информации (FIPS)	• Соответствие FIPS 140-2 уровня 2 (применяются ограничения по платформе, функциональности и версии).
Защищенная мобильность и мониторинг сети	
Интеграция возможности защиты веб-трафика (необходима лицензия на облачное устройство защиты веб-трафика)	• Использование облачного устройства защиты веб-трафика, крупнейшего глобального решения для защиты веб-трафика по модели «программное обеспечение как услуга (SaaS)» для защиты корпоративных сетей от вредоносных программ и контроля и защиты веб-трафика, потребляемого пользователем. • Поддерживает облачные конфигурации и динамическую нагрузку. • Обеспечивает для организаций гибкость и возможность выбора благодаря поддержке облачных сервисов, помимо локальных. • Интегрируется с физическим устройством защиты веб-трафика. • Поддерживает обнаружение доверенных сетей. • Обеспечивает принудительное применение политик в каждой транзакции, независимо от местонахождения пользователя. • Требует всегда работающего сетевого подключения с высоким уровнем безопасности и действующей политикой для разрешения или запрета подключения к сети в случае, если доступ становится невозможен. • Обнаруживает общую точку доступа и связанные порталы.
Cisco Umbrella Roaming (необходима лицензия Cisco Umbrella Roaming)	• Обеспечивает безопасность устройств в роуминге при отключенном VPN-доступе. • Автоматические блокирует вредоносное ПО, фишинговые атаки и обратные вызовы C2 на устройствах в роуминге. • Представляет собой простейший способ защиты устройств в любом месте. • Использует перенаправление трафика оконечных устройств для обеспечения безопасности на основе протоколов DNS при отключенном VPN-доступе или с раздельными туннелями (применяется для подключений за пределами туннеля).
Модуль мониторинга сети (Требуется лицензия Apex.)	• Захват потоков оконечных устройств с подробным контекстными данными о пользователе, оконечном устройстве, приложении, местоположении и адресе назначения. • Гибкие настройки сбора данных локально и удаленно. • Выявление потенциальных аномалий в поведении благодаря мониторингу использования приложений. • Возможность принятия более обоснованных решений. • Возможность передачи данных об использовании приложений в самые разные инструменты сетевого анализа с поддержкой Internet Protocol Flow Information Export (IPFIX).
Решение Advanced Malware Protection (AMP) for Endpoints Enabler (требуется отдельная лицензия на AMP for Endpoints)	• Упрощает активацию сервисов зашиты от угроз для оконечных устройств AnyConnect за счет распределения и подключения Cisco AMP для оконечных устройств. • Обеспечивает защиту от угроз удаленных оконечных устройств, обеспечивая больший охват оконечных устройств для защиты их от угроз. • Обеспечивает более проактивную защиту, чтобы гарантировать быстрое устранение угрозы на удаленном оконечном устройстве.

Функция	Преимущества и описание
Поддержка широкого спектра операционных систем	• Windows 10, 8.1, 8 и 7 • Mac OS X 10.8 или выше
Network Access Manager и 802.1X	
Поддержка медиатехнологий	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
Аутентификация сети	• IEEE 802.1X-2001, 802.1X-2004 и 802.1X-2010 • Обеспечивает предприятиям возможность развертывать единую структуру аутентификации 802.1X для доступа и к проводным, и к беспроводным сетям. • Управляет идентификацией пользователей и устройств и протоколами сетевого доступа, требуемыми для доступа с высоким уровнем безопасности. • Обеспечивает удобную работу пользователя при подключении к унифицированной проводной и беспроводной сети Cisco.
Протокол расширенной аутентификации (Extensible Authentication Protocol, EAP).	• Протокол EAP-Transport Layer Security (TLS) • Протокол EAP-Protected Extensible Authentication Protocol (PEAP) со следующими протоколами внутри туннеля: o EAP-TLS; o EAP-MSCHAPv2. o Протокол EAP-Generic Token Card (GTC) • Протокол гибкой аутентификации через защищенное туннелирование (EAP-Flexible Authentication via Secure Tunneling, FAST) со следующими протоколами внутри туннеля: o EAP-TLS; o EAP-MSCHAPv2; o EAP-GTC. • Протокол EAP-Tunneled TLS (TTLS) со следующими протоколами внутри туннеля: o протокол аутентификации по паролю (Password Authentication Protocol, PAP); o протокол аутентификации по запросу при установлении связи (Challenge Handshake Authentication Protocol, CHAP); o Microsoft CHAP (MSCHAP); o MSCHAPv2; o EAP-MD5; o EAP-MSCHAPv2; • облегченный протокол EAP (LEAP), только Wi-Fi; • EAP-Message Digest 5 (MD5), конфигурируется администратором, только Ethernet; • EAP-MSCHAPv2, конфигурируется администратором, только Ethernet; • EAP-GTC, конфигурируется администратором, только Ethernet.
Способы шифрования беспроводного доступа (требуется поддержка соответствующего стандарта 802.11 NIC)	• Открытые. • Протокол безопасности, аналогичной защите проводной сети (Wired Equivalent Privacy, WEP). • Динамический WEP. • Защищенный доступ Wi-Fi (WPA) для предприятий. • WPA2 для предприятий. • WPA для личного пользования (WPA-PSK). • WPA2 для личного пользования (WPA2-PSK). • CCKM (требуется Cisco CB21AG Wireless NIC).
Протоколы шифрования беспроводного доступа	• Режим гаммирования с протоколом Cipher Block Chaining Message Authentication Code Protocol (CCMP) и с симметричным алгоритмом блочного шифрования Advanced Encryption Standard, AES. • Протокол шифрования с использованием временных ключей (Temporal Key Integrity Protocol, TKIP) с использованием поточного шифрования Rivest Cipher 4 (RC4).
Возобновление сеанса	• Возобновление сеанса RFC2716 (EAP-TLS) с использованием EAP-TLS, EAP-FAST, EAP-PEAP и EAP-TTLS. • Возобновление сеанса EAP-FAST без сохранения состояния. • Кэширование PMK-ID [проактивное кэширование ключей (Proactive Key Caching, PKC) или гибкое кэширование ключей (Opportunistic Key Caching, OKC)], только Windows XP.
Шифрование Ethernet	• Управление доступом к передающей среде: IEEE 802.1AE (MACsec). • Управление ключами: MACsec Key Agreement (MKA) • Определяет инфраструктуру безопасности в проводной сети Ethernet для обеспечения конфиденциальности и целостности данных, а также аутентификации происхождения данных. • Обеспечивает защищенные коммуникации между доверенными компонентами сети.
Одно подключение в один момент времени	• Разрешает только одно подключение к сети, отсоединяя при этом все остальные подключения. • Отсутствие мостового соединения между адаптерами. • Подключения по Ethernet автоматически получают приоритет.
Комплексная проверка сервера	• Поддерживает правила «заканчивается с» и «точное совпадение». • Поддерживает более 30 правил для серверов без унификации имен.
Создание цепочки EAP (EAP-FASTv2)	• Дифференцирует доступ на основе активов (корпоративные или не корпоративные). • Выполняет подтверждение пользователей и устройств в одной транзакции EAP.
Обеспечение корпоративного подключения (ECE)	• Обеспечивает подключение пользователей только к соответствующей корпоративной сети. • Предотвращает подключение пользователей к сторонней точке доступа в целях использования Интернета в офисе. • Предотвращает подключение пользователей к гостевой сети. • Исключает создание объемных черных списков.

Функция	Преимущества и описание
Шифрование нового поколения (Suite B)	• Поддерживает самые последние криптографические стандарты. • Протокол обмена ключами Диффи-Хеллмана на основе эллиптических кривых (Elliptic Curve Diffie-Hellman key exchange, ECDHKE). • Сертификаты алгоритма сигнатур на основе эллиптических кривых (Elliptic Curve Digital Signature Algorithm, ECDSA).
Типы учетных данных	• Интерактивные пароли пользователя или пароли Windows. • Токены RSA SecurID. • Токены одноразовых паролей (OTP). • Смарт-карты (Axalto, Gemplus, SafeNet iKey, Alladin). • Сертификаты X.509. • Сертификаты алгоритма сигнатур на основе эллиптических кривых (Elliptic Curve Digital Signature Algorithm, ECDSA).
Удаленная поддержка настольных ПК	• Аутентификация учетных данных удаленных пользователей в локальной сети при использовании протокола удаленного рабочего стола (Remote Desktop Protocol, RDP).
Поддерживаемые операционные системы	• Windows 10, 8.1, 8 и 7.

Совместимость с платформами

Решение AnyConnect совместимо со всеми моделями корпоративных версий межсетевых экранов Cisco ASA серий 5500-X и 5500 нового поколения, поддерживающих версию ПО Cisco ASA 8.0(4) или более позднюю. Рекомендуется развертывать текущие версии программного обеспечения устройства.

Отдельные функции доступны только на более поздних версиях ПО Cisco ASA или моделях ASA 5500-X.

Cisco поддерживает VPN-доступ AnyConnect к ОС Cisco IOS® версии 15.1(2)T и более поздним, функционирующим в качестве шлюза безопасности с определенными ограничениями функционала. Более подробную информацию см. в разделе Функции, не поддерживаемые Cisco IOS SSL VPN.

Дополнительную информацию о поддержке функций 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.

Варианты лицензирования

- Для AnyConnect версии 4.x или более поздней требуются лицензии AnyConnect Plus или Apex.
- Информацию о вариантах лицензирования и оформлении заказа можно посмотреть в руководстве по оформлению заказов 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.
- Информационный бюллетень Cisco AnyConnect для мобильных платформ: http://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/data_sheet_c78-527494.html.
- Многофункциональные устройства обеспечения безопасности Cisco ASA 5500-X: http://www.cisco.com/go/asa.
- Облачная система обеспечения безопасности веб-трафика Cisco Cloud Web Security http://www.cisco.com/go/cws.
- Cisco AMP для оконечных устройств http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html.
- Лицензионное соглашение и политика конфиденциальности для Cisco AnyConnect: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
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, www.cisco.com

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 этаж
Телефон: +994 (12) 437 4820, 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