Платформа Cisco Identity Services Engine

В связи с увеличением количества пользователей, устройств и методов доступа корпоративные ИТ-инфраструктуры современных предприятий становятся более динамичными. Наряду с расширением возможных вариантов подключения и спектра пользовательских устройств появляются новые риски нарушения безопасности и задачи по сохранению управляемости. Для обеспечения информационной безопасности корпоративной ИТ-инфраструктуры и эффективного управления такой инфраструктурой требуются новые решения, которые обеспечат выполнение политик доступа, аудит доступа к ИТ-инфраструктуре, мониторинг соблюдения нормативных требований, а также сбор подробных сведений о всех сетевых взаимодействиях.

Компания Cisco разработала решение, призванное упростить деятельность специалистов по сетевой безопасности и администраторов сети, — Cisco® Identity Services Engine.

Обзор продукта

Cisco Identity Services Engine является платформой следующего поколения для управления процессами идентификации и контроля доступа, которая позволяет организациям обеспечить соблюдение нормативных требований, повысить уровень защищенности корпоративной ИТ-инфраструктуры и упростить управление работой сетевых сервисов. Благодаря уникальной архитектуре решения предприятия могут в режиме реального времени получать из сетей, от пользователей и устройств контекстную информацию, необходимую для принятия упреждающих решений по предоставлению доступа. Все решения принимаются на основании единой политики доступа, распространяющейся на проводные сегменты сети, беспроводные сегменты сети и подключения удаленного доступа. Cisco Identity Services Engine является неотъемлемым компонентом решения Cisco TrustSec® и архитектуры Cisco SecureX.

Cisco Identity Services Engine представляет собой высокопроизводительное и гибкое решение для контроля доступа с учетом контекста, которое объединяет сервисы аутентификации, авторизации и учета (AAA), оценки состояния, профилирования и управления гостевым доступом в рамках единой платформы. Администраторы получают возможность централизованно создавать согласованные политик контроля доступа и управления ими, а также полную осведомленность обо всех пользователях и устройствах, подключающихся к сети. Решение Cisco Identity Services Engine автоматически выявляет и классифицирует оконечные устройства, обеспечивает нужный уровень доступа, проводя аутентификацию как пользователей, так и устройств, а также обеспечивает соответствие оконечных устройств нормативным требованиям путем оценки их состояния защищенности перед предоставлением доступа к корпоративной ИТ-инфраструктуре. Cisco Identity Services Engine поддерживает гибкие механизмы контроля доступа, включая группы безопасности (SGA), метки групп безопасности (SGT) и списки контроля доступа групп безопасности (SGACL).

Функциональные возможности и преимущества

Являясь неотъемлемым компонентом решения Cisco TrustSec, платформа Cisco Identity Services Engine предоставляет следующие возможности.

- Внедрение в корпоративную ИТ-инфраструктуру средств аутентификации и авторизации пользователей и оконечных устройств, подключенных к проводным сетям, беспроводным сетям и сетям VPN, обеспечение соблюдения согласованной политики в масштабах всего предприятия.
- Предотвращение несанкционированного доступа к сети для защиты корпоративных активов.
- Управление полным жизненным циклом гостевого доступа за счет предоставления приглашающим лицам (спонсорам) средств для разрешения доступа их гостей, что позволяет снизить текущую нагрузку на ИТ-специалистов.
- Поддержка настраиваемых порталов и возможности публикации web-страниц для упрощения работы как новых, так и опытных пользователей в соответствии с принятыми в организации процессами.
- Обеспечение полномасштабного мониторинга путем обнаружения, классификации и управления подключающимися к сети оконечными устройствами для предоставления соответствующих сервисов и уровней доступа.
- Устранение уязвимостей на компьютерах пользователей путем регулярной проверки и корректировки их состояния, что позволяет нейтрализовать такие сетевые угрозы, как вирусы, черви и шпионские программы.
- Обеспечение соблюдения политик безопасности за счет блокировки и изоляции несоответствующих корпоративным стандартам компьютеров в карантинной области, а также их обновления без привлечения администратора.
- Поддержка встроенной консоли мониторинга, отчетности и устранения неполадок для упрощения работы специалистов службы поддержки и администраторов.
- Повышение точности профилирования подключенных к сети устройств за счет методов активного сканирования устройства. Этот механизм позволяет повысить точность профилирования устройств, для которого раньше использовались только средства анализа сетевого трафика, за счет сканирования определенных атрибутов устройства (в соответствии с политикой).
- Управление доступом оконечных устройств к сети с помощью сервиса защиты оконечных устройств (EPS). Сервис EPS позволяет администратору связывать оконечные устройства и действия, которые необходимо выполнить при подключении устройства (перенос в новую VLAN, возврат в исходную VLAN или полная изоляция устройства от сети), с помощью единого интерфейса.

Cisco Identity Services Engine предоставляют ряд дополнительных основных возможностей, которые описаны в таблице 1.

Таблица 1. Основные функциональные возможности платформы Cisco Identity Services Engine

Функциональная возможность	Описание
Протоколы AAA	Использование стандартного протокола RADIUS для аутентификации, авторизации и учета (AAA).
Протоколы аутентификации	Поддерживает широкий диапазон протоколов аутентификации, включая PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST) и EAP-Transport Layer Security (TLS).
Модель политики	Поддерживает модель политики на основе правил и условий для создания гибких и важных для бизнеса политик контроля доступа. Позволяет задавать политики путем извлечения атрибутов из заранее определенных баз, в которых содержатся данные об учетных данных пользователей и оконечных устройств, оценке состояния, протоколах аутентификации, результатах профилирования и т. д. Атрибуты можно создать динамически и сохранить для использования в дальнейшем.

Таблица 1. Основные функциональные возможности платформы Cisco Identity Services Engine (*продолжение*)

Функциональная возможность	Описание
Контроль доступа	Поддерживает множество различных механизмов контроля доступа, включая загружаемые списки контроля доступа (dACL), назначение сетей VLAN, перенаправление по URL-адресам и добавление меток SGA, что позволяет использовать расширенные возможности сетевых устройств Cisco.
Профилирование	В базе данных платформа содержатся предопределенные шаблоны устройств для различных оконечных устройств, таких как IP-телефоны, принтеры, IP-камеры, смартфоны и планшеты. Администраторы могут создавать собственные шаблоны устройств. Их можно использовать для автоматического обнаружения, классификации и связывания определенных администраторами идентификационных данных при подключении оконечных устройств к сети. Кроме того, администраторы могут задавать политики авторизации на основе типа устройства. Платформа Cisco Identity Services Engine собирает сведения об атрибутах оконечных устройств с использованием средств пассивной сетевой телеметрии, путем активного сканирования оконечных устройств, а также путем взаимодействия с сенсорами устройств, функционирующими на коммутаторах Cisco Catalyst. Средства профилирования устройств, размещенные на коммутаторах Cisco Catalyst, являются одним из элементов технологии профилирования Cisco ISE. Они позволяют коммутаторам быстро собрать сведения об оконечных устройствах, подключенных к ним, и передать собранные сведения по протоколу RADIUS платформе Cisco ISE для классификации устройств и назначения соответствующих политик. Технология профилирования с использованием сенсоров на коммутаторах позволяет осуществить эффективный сбор сведений об оконечных устройствах в рамках распределенной ИТ-инфраструктуры, а также обеспечивает масштабируемость платформы, упрощает развертывание и позволяет повысить эффективность классификации устройств.
Управление жизненным циклом гостевого доступа	Платформа обеспечивает управление полным жизненным циклом гостевого доступа, при котором пользователи со статусом «Гость» могут получить контролируемый доступ к сети в течение ограниченного времени при поддержке администратора или путем самостоятельной регистрации на портале гостевого доступа. Позволяет администраторам настраивать порталы и политики с учетом конкретных потребностей организации.
Оценка состояния оконечных устройств	Проводит оценку состояния оконечных устройств для всех типов пользователей, подключающихся к сети. Функционирует с использованием либо постоянно установленного на устройстве агента, либо с использованием временно загружаемого web-агента. В процессе оценки состояния оконечных устройств оценивается соответствие оконечного устройства требованиям политик безопасности, таким как наличие последних исправлений для операционных систем и наличие пакета антивирусного программного обеспечения с самыми последними и актуальными антивирусными базами. Развитая система оценки состояния оконечных устройствах позволяет выполнять проверку файловых переменных (версия, дата и т. д.), реестра (раздел, значение и т. д.) и приложений. Чтобы гарантировать соответствие оконечного устройства политикам компании, платформа Cisco ISE обеспечивает регулярное автоматическое обновление клиента и проводит повторную оценку состояния устройства.
Сервис защиты оконечных устройств	Позволяет администраторам оперативно предпринимать корректирующие меры (помещение в карантин, вывод из карантина и полное блокирование) к оконечным устройствам, не соответствующим требованиям политик безопасности. Это позволяет снизить риски и повысить уровень защищенности всей ИТ-инфраструктуры.
Централизованное управление	Позволяет администраторам централизованно настраивать сервисы профилирования, оценки состояния, гостевого доступа и авторизации и управлять ими с помощью единой web-консоли с графическим интерфейсом, значительно упрощая администрирование за счет согласованного управления всеми сервисами.
Мониторинг и устранение неполадок	Включает интегрированный компонент мониторинга, отчетности и устранения неполадок, доступный с помощью графического web-интерфейса и предназначенный для упрощения работы сотрудников службы поддержки и операторов сетей. Предлагает средства формирования комплексной отчетности для всех сервисов, регистрации всех действий, а также отслеживание в режиме реального времени всех пользователей и оконечных устройств, подключающихся к сети, с помощью панели мониторинга.
Варианты платформы	Поставляется в формате физического или виртуального устройства. Поддерживаются три платформы физического устройства, а также виртуальная машина для среды VMware ESX или ESXi.

Преимущества

Платформа Cisco Identity Services Engine характеризуется следующими преимуществами.

- Эта платформа позволяет организациям выполнять согласованное развертывание сложных индивидуализированных бизнес-политик доступа.
- Платформа позволяет снизить операционные расходы за счет обеспечения полного мониторинга, формирования исторических отчетов и расширенных средств поиска и устранения неполадок сетевого доступа.
- Платформа позволяет уменьшить число перебоев в работе сети и сократить время простоя за счет того, что доступ к сети предоставляется только пользователям, соответствующим требованиям политик, а пользователи, которые не соответствуют требованиям политик, изолируются в отдельные области сети с ограниченным доступом к корпоративным ИТ-ресурсам.
- Платформа позволяет организациям обеспечить соответствие нормативным требованиям, поскольку она обеспечивает реализацию необходимых механизмов обеспечения информационной безопасности и их аудит.

Технические характеристики продукта

Существует три варианта аппаратной платформы Cisco Identity Services Engine (см. таблицу 2).

Таблица 2. Технические характеристики устройства Cisco Identity Services Engine

	Cisco Identity Services Engine Appliance 3315 (начальная)	Cisco Identity Services Engine Appliance 3355 (средняя)	Cisco Identity Services Engine Appliance 3395 (мощная)
Процессор	1 четырехъядерный ЦП Intel Core 2 Q9400, 2,66 ГГц	1 четырехъядерный ЦП Intel Xeon E5504, 2 ГГц	2 четырехъядерных ЦП Intel Xeon E5504, 2 ГГц
Память	4 Гбайт	4 Гбайт	4 Гбайт
Жесткий диск	2 жестких диска SATA емкостью 250 Гбайт каждый	2 накопителя SAS емкостью 300 Гбайт каждый	4 накопителя SFF SAS емкостью 300 Гбайт каждый
RAID	Нет	Да (RAID 0)	Да (RAID 0+1)
Дисковод	CD/DVD-ROM	CD/DVD-ROM	CD/DVD-ROM
Сетевые подключения			
Ethernet-адаптеры	4 интегрированных адаптера Gigabit Ethernet	4 интегрированных адаптера Gigabit Ethernet	4 интегрированных адаптера Gigabit Ethernet
Поддержка кабеля 10BASE-T	Неэкранированная витая пара (UTP) категории 3, 4 или 5, до 328 футов (100 м)	Неэкранированная витая пара (UTP) категории 3, 4 или 5, до 328 футов (100 м)	Неэкранированная витая пара (UTP) категории 3, 4 или 5, до 328 футов (100 м)
Поддержка кабеля 10/100/1000BASE-TX	Неэкранированная витая пара (UTP) категории 5, до 328 футов (100 м)	Неэкранированная витая пара (UTP) категории 5, до 328 футов (100 м)	Неэкранированная витая пара (UTP) категории 5, до 328 футов (100 м)
Плата ускорителя SSL	Нет	Cavium CN1620-400-NHB-G	Cavium CN1620-400-NHB-G
Интерфейсы			
Последовательные порты	1	1	1
Порты USB 2. 0	4 (два спереди, два сзади)	4 (один спереди, один внутри, два сзади)	4 (один спереди, один внутри, два сзади)
Видеопорты	1	1	1
Внешние порты SCSI	Нет	Нет	Нет

Таблица 2. Технические характеристики устройства Cisco Identity Services Engine (*продолжение*)

	Cisco Identity Services Engine Appliance 3315 (начальная)	Cisco Identity Services Engine Appliance 3355 (средняя)	Cisco Identity Services Engine Appliance 3395 (мощная)
Системный блок			
Размер	1 RU, для монтажа в стойку	1 RU, для монтажа в стойку	1 RU, для монтажа в стойку
Масса	28 фунтов (12,7 кг) в полной комплектации	35 фунтов (15,87 кг) в полной комплектации	35 фунтов (15,87 кг) в полной комплектации
Габариты	1,69 x 17,32 x 22 дюйма (4,3 x 44 x 55,9 см)	1,69 x 17,32 x 27,99 дюйма (43 x 42,62 x 71 см)	1,69 x 17,32 x 27,99 дюйма (43 x 42,62 x 71 см)
Блок питания	350 Вт	2 по 675 Вт (резервируемые)	2 по 675 Вт (резервируемые)
Вентиляторы системы охлаждения	6, без «горячего» подключения, без резервирования	9, резервируемые	9, резервируемые
Показатель БТЕ	1024 БТЕ/час (при 300 Вт)	2661 БТЕ/час (при 120 В)	2661 БТЕ/час (при 120 В)

Виртуальные устройства Cisco Identity Services Engine поддерживаются в VMware ESX/ESXi 4.x. Их следует запускать на оборудовании, характеристики которого соответствуют характеристикам устройств, приведенным в таблице 2, или превосходят их. Минимальные требования к виртуальной машине – это объем оперативной памяти не менее 4 Гбайт памяти и не менее 200 Гбайт пространства на жестком диске. Виртуальная машина соответствует требованиям сертификации FIPS140-2 уровня 1.

Системные требования

Системные требования программного обеспечения Cisco NAC Agent, реализующего проверку состояния оконечных устройств, приведены в таблице 3.

Таблица 3. Системные требования к Cisco NAC Agent

Компонент	Минимальные требования
Поддерживаемая ОС	Microsoft Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE и Windows ME; Mac OS X (v10.5.x, v10.6.x)
Пространство на жестком диске	Минимум 10 Мбайт свободного места на жестком диске
Оборудование	Минимальные требования к оборудованию отсутствуют (работает на различных клиентских компьютерах)

Спецификации лицензий

Для активации различных сервисов при развертывании платформы Cisco Identity Services требуется лицензия. В настоящее время поддерживаются лицензии на использование платформы Cisco Identity Services трех типов.

- **Лицензия ISE BASE.** Используется для активации базовых сервисов, таких как сервисы аутентификации, авторизации, гостевого доступа, мониторинга и устранения неполадок.
- **Лицензия ISE ADVANCED.** Используется для активации расширенных сервисов, таких как оценка состояния оконечного узла, сервис профилирования, поддержки SGA и EPS. Обратите внимание, что для установки лицензии ISE ADVANCED требуется лицензия ISE BASE.
- **Лицензия ISE WIRELESS.** Позволяет активировать все сервисы ISE, но только для устройств, подключенных к беспроводной сети.

Обзор различных лицензий представлен в таблице 4.

Таблица 4. Характеристики лицензий на использование платформы Cisco Identity Services Engine

	Лицензия BASE	Лицензия ADVANCED	Лицензия WIRELESS
Аутентификация и авторизация	X		X*
Сервисы гостевого доступа	X		X*
Мониторинг и устранение неполадок	X		X*
Оценка состояния оконечных устройств		X	X*
Профилирование		X	X*
Поддержка SGA		X	X*
Сервис защиты оконечных устройств		X	X*

* Только для оконечных устройств, подключенных к беспроводной сети

Обслуживание и техническая поддержка

Компания Cisco предлагает широкий диапазон программ по обслуживанию и поддержке, которые призваны содействовать успеху бизнеса заказчиков. Эти передовые программы реализуются благодаря уникальному сочетанию человеческих ресурсов, процессов, инструментов и партнеров, что позволяет полностью удовлетворять запросы заказчиков. Услуги Cisco помогают защитить ваши инвестиции в организацию сетей, оптимизировать работу сетей и подготовить их для реализации новых приложений, расширяющих интеллектуальные функции сетей и повышающих эффективность вашего бизнеса. Для получения более подробной информации об услугах Cisco, обращайтесь в подразделение Cisco Technical Support Services (услуги по технической поддержке) или Cisco Advanced Services (услуги технического консалтинга).

Сведения об условиях гарантии см. на web-странице http://www.cisco.com/go/warranty. Сведения о лицензировании доступны на web-странице http://www.cisco.com/en/US/docs/security/nac/appliance/support guide/license.html.

Дополнительная информация

Для получения дополнительных сведений о продуктах семейства Cisco Identity Services Engine и решении Cisco TrustSec посетите сайт по адресу http://www.cisco.com/go/ise или обратитесь к представителю Cisco по работе с заказчиками.

Cisco
Россия, 115054, Москва,
Космодамианская наб.,
52, стр.1, 4 этаж
Телефон: +7 495 9611410
Факс: +7 495 9611410
www.cisco.ru
www.cisco.com

Cisco
Россия, 197198,
Санкт-Петербург,
пр. Добролюбова, 16, лит. А, кор. 2
Телефон: +7 812 3136230
Факс: +7 812 3136280
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038,
Киев,
ул.Николая Гринчинко, 4В
Тел: +38 044 3913600
Факс: +38 044 3913601
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 050059, Алматы,
Ул. О. Жолдасбекова, 97,
блок А2, 14 этаж
Телефон: +7 727 2442101
Факс: +7 727 244 2102
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**