NAC: безопасность по принуждению

Проблема безопасного доступа к корпоративной сети сегодня очень остро стоит перед компаниями любого уровня. Утечка критически важной корпоративной информации, рост объемов паразитного трафика, вымогательство, шантаж и заказные атаки на информационные ресурсы конкурентов — рано или поздно такие события обязательно произойдут там, где есть малейшая лазейка для доступа в сеть. В условиях постоянного совершенствования информационных угроз и быстрого роста числа мобильных устройств технология NAC занимает особое место в реализации стратегии защиты информационной инфраструктуры компании.

Архитектура системы защиты обычно разрабатывается на основе управления рисками (Risk Management) и ориентирована на достижение баланса между ценностью информации и размером инвестиций в ее защиту. Абсолютной защиты не существует, к тому же угрозы постоянно меняются: многие эксперты в области информационной безопасности отмечают, что совершенная защита невозможна даже теоретически. Поэтому основные баррикады должны возводиться в первую очередь там, где потенциал риска особенно высок. Ситуаций, когда подключение пользователя к сети компании может подвергнуть риску его репутацию и даже доходы, очень много. Потенциальную опасность заражения сети вредоносным кодом таит в себе не только подключаемый к ней ноутбук посетителя, но и рабочая станция с просроченной лицензией на компьютере штатного сотрудника.

В последние годы все более заметное место на рынке занимает эффективная стратегия защиты посредством контроля доступа к сети и ее ресурсам — технология NAC.

Рынок NAC растет довольно быстрыми темпами, хотя эксперты и для него предсказывают

непростые времена. По мнению Gartner, несмотря на консолидацию вендоров и уход с этого рынка некоторых игроков, неплохие шансы остаются даже у начинающих компаний. По данным этого аналитического агентства, в 2007 году доходы от продажи инструментов NAC выросли на 90%, а в 2008-м — на 50% (Gartner предсказывал рост в прошлом году на уровне 100%). Из наиболее известных в мире производителей NAC российский рынок знаком с продукцией Cisco, Microsoft, Symantec и Juniper. На мировом рынке в этой нише также широко представлено комплексное решение компании Trusted Network Control (TNC), но в нашей стране оно практически неизвестно. С той или иной степенью полноты элементы NAC присутствуют в продуктах таких компаний, как Hewlett Packard, Extreme, McAfee, Check Point, LanDesk.

Что такое NAC?

Для обозначения динамично эволюционирующей технологии контроля доступа к сети в отрасли уже сложилось устоявшееся название Network Access Control, NAC, хотя у разных вендоров оно варьируется.

В терминологии Symantec аббревиатура NAC расшифровывается как Network Access Control, Microsoft интерпретирует ее как Network Access Protection, в варианте Juniper это Networks Unified Access Control, а у Cisco Systems — Network Admission Control. Есть и другие названия одного и того же понятия: Trusted Access, Total Access Protection и даже Network Node Validation. В любом случае, несмотря на то что на рынке не существует стандарта NAC, суть этой стратегии защиты сводится к регламенту доступа пользователей к сети и постоянному контролю над состоянием конечных сетевых устройств — как внутренних сотрудников, так и удаленных, и в том числе мобильных пользователей.

«Первоначальная идея NAC заключалась в том, чтобы предоставить или ограничить доступ клиента к сети — в зависимости о его «здоровья», — говорит Константин Троицкий — руководитель технического отдела компании «Поликом Про». — Сегодня роль NAC состоит в соответствии политикам как критерию для принятия решений и совершения действий».

Технология NAC реализует широкий перечень функций, которые охватывают идентификацию пользователей, оценку и идентификацию состояния конечных точек, меры по пресечению угроз, проверку устройств на соответствие корпоративным политикам доступа в сеть. «Решая вопросы безопасности подключения пользовательских устройств в комплексе, технология NAC вторглась в сферу ответственности сразу трех подразделений — ИТ, ИБ и сетевого — и стала их общей головной болью, несмотря на разные задачи, которые решают эти структуры», — отмечает Михаил Орешин, директор московского офиса компании «Поликом-Про». — Но у одной системы не может быть трех хозяев. Хотя однозначных рекомендаций не существует, очевидно, кто-то должен взять ее под свою ответственность, так чтобы остальные могли пользоваться этой функциональностью».

На раннем этапе развития NAC методы контроля подключений персональных устройств к сети реализовались на основе протокола 802.1x и при этом были чрезвычайно сложны для внедрения и поддержки в масштабных сетях. Для контроля не было приспособленных механизмов, отсутствовали обратная связь и отчетность. Для реализации карантина различные вендоры предлагали спорные механизмы, а конфигурация доступа клиентов представлялась сложной.

— 802.1x появился в 2001 году в целях контроля подключений персональных устройств в беспроводных сетях, — поясняет Виталий Томилко, технический руководитель направления «Корпоративные сети» компании «Открытые ?Технологии». — Алгоритм 802.1x решает задачи контроля сетевого доступа лишь на втором и третьем уровнях модели OSI — закрывает доступ к проводной или беспроводной сети на уровне «порта подключения». В настоящее время существует тенденция отказа от протокола 802.1x, поскольку он никак не контролирует происходящего на рабочих станциях. Два подхода —

на основе агентского ПО и на основе 802.1x, — несмотря на возможность совмещения, на практике взаимно исключают друг друга. Например, решение Cisco Clean Access никак не связано с 802.1x.
Как поясняет Виталий Томилко, существует удобная интеграция 802.1x с платформой Microsoft Active Directory, благодаря чему можно контролировать подключение пользователей или сетевых устройств к сети. Применение системы контроля доступа на основе протокола 802.1x позволит
– контролировать подключение пользователей или устройств к сети (идентифицировать, назначить в определенный VLAN, присвоить соответствующий IP-адрес);
– собирать статистику: какой пользователь, когда, на каком коммутаторе, с каким IP-адресом произвел подключение к сети. Опционально — сколько времени проработал, какую нагрузку на сеть произвел;
– предоставить гостевой вход в Интернет для рабочих станций заказчиков и партнеров, находящихся на территории организации;
– обеспечить подключение принтеров, терминалов и других устройств, не поддерживающих 802.1x.
Тем самым применение 802.1x гарантирует, что в сети никогда не появится неавторизованное устройство. Однако не следует забывать, что при 802.1x контроль доступа к съемным носителям и проверка программного обеспечения подключаемых устройств не поддерживаются. А ведь именно эти два фактора являются причиной возникновения большинства инцидентов (утечка информации, распространение вирусов в локальной сети и др.). С развитием второго поколения систем контроля доступа к сети пришли и решения, основанные на использовании агента, который контролирует целостность программной среды и процессов, протекающих на рабочих станциях. Уже на этом уровне возникает вопрос профилирования различных пользователей и применения к ним различных политик доступа.

Колонка Эксперта

Владимир Баланин, руководитель отдела ИТ-безопасности компании TopS BI (Группа «Систематика»)

Изначально технология NAC разрабатывалась для сканирования клиентских устройств относительно таких критериев безопасности, как наличие антивирусного ПО, обновлений ОС и т. д. В случае нарушения данных критериев NAC позволяет изолировать потенциально опасное устройство до устранения обнаруженных уязвимостей. Однако мир не стоит на месте, и технология NAC за время ее существования трансформировалась из простой проверки и изоляции оконечных устройств в так называемый compliance checking. Я бы даже позволил себе сказать, что технология NAC стала хорошим правилом «сетевой гигиены».
Существует немалое количество разработчиков (Microsoft, Cisco, Juniper, Symantec, McAfee и т. д.) предлагающих различные версии NAC и с различным функционалом — от простых правил «разрешить/запретить» до предоставления автоматических методов по устранению несоответствий политики безопасности. При этом разработчики предлагают собственные (proprietary) реализации NAC, и единственное, что их объединяет, — это три общих подхода к реализации технологии:
• программный агент, устанавливаемый на конечное оборудование;
• инфраструктурные решения;
• программно-аппаратные комплексы (appliance) (ПАК).
Очевидно, что ПАК являются наиболее простым и дешевым решением, но они имеют ряд

функциональных ограничений, поэтому чаще всего используются «гибриды» — комбинация указанных выше решений (и, возможно, от разных вендоров). Какая комбинация будет использована в каждом конкретном случае, на мой взгляд, зависит в первую очередь от размера компании. Для небольшой фирмы наиболее вероятным выбором будет комбинация ПАК и программных агентов, а для крупной (более тысячи рабочих мест) — ПАК и инфраструктурные решения.
Хотя основными при внедрении NAC считаются проблемы интеграции, комплексность решений и сложность их внедрения, многих трудностей можно избежать, если подход будет более «бизнес-ориентированным». К примеру, если первичной целью внедрения NAC было управление гостевым доступом, а через некоторый промежуток времени было принято решение о внедрении ролевой модели доступа (RBAC) для сотрудников, то, возможно, первоначальные инвестиции просто пропадут, так как весьма вероятно, что «идеальное» решение для первоначальной задачи окажется «посредственным» при выполнении второй. Поэтому необходимо еще перед принятием решения о внедрении NAC определить несколько возможных сценариев использования технологии. Причем их должно быть не много — 2-4, иначе сроки внедрения могут значительно превысить планируемые — или, как самый плохой вариант, внедрение не будет признано успешным.
Стоит отметить: несмотря на то что первое слово в аббревиатуре NAC — Network, для успешного внедрения NAC необходимо тесное взаимодействие трех подразделений — сетевого, информационной безопасности и ИТ. При этом каждое подразделение решает свои задачи:
• сетевое — оценка возможностей существующей инфраструктуры, разработка решения и его внедрение;
• информационная безопасность — разработка и применение политик доступа;
• ИТ — разработка и обеспечение процесса устранения обнаруженных несоответствий политике безопасности, даже несмотря на то, что многие решения NAC позволяют устранять обнаруженные проблемы в автоматическом режиме.

Еще хотелось бы дополнительно обсудить тему «Compliance» (соответствие политикам, законодательству, стандартам…), но применительно не к внутренним политикам, а к требованиям различным стандартов. Некоторые вендоры могут утверждать, что для соответствия таким стандартам, как PCI DSS, SOX, просто необходимо внедрить технологию NAC. На самом деле это не так, хотя нужно признать, что внедрение NAC может упростить получение заветной «галочки» у аудитора. Если посмотреть на требования PCI DSS, SOX с точки зрения «сети», то должны выполняться пять следующих положений:
• наличие политик безопасности;
• аутентификация пользователей;
• контроль доступа;
• возможность реагирования на инциденты ИБ путем оповещения заинтересованных сторон и применения мер контроля для изоляции проблемы;
• аудит использования систем и факта доступа к конфиденциальной информации.
Конечно, NAC не сможет помочь в написании политик безопасности, но положения со второго по четвертое с его помощью реализуются. Аудит технологией NAC также не обеспечивается, но NAC может быть ценным источником данных для внешних систем протоколирования и отчетности.

Найти и обезвредить
Эксперты выделяют пять основных функций, которые являются частью продуктов NAC. Это
— оценка состояния конечных точек до их подключения к сети;

— изоляция конечных точек в карантине и комплекс мер по их «излечению»;
— контроль доступа к сети на основе идентификации пользователей;
— контроль сетевых ресурсов на основе идентификации и политик;
— непрерывный анализ угроз и их предотвращение.
Идентификация подключающихся конечных точек сводится к ответу на вопросы: кто, где, каким способом. Организация доступа к ресурсам по ролям обеспечивает доступ только к тому, что необходимо. Контроль же исполнения корпоративных политик сводится к принудительному соответствию.
«Я бы рассматривал NAC, — говорит Виталий Томилко, — как стратегию, воплощение которой позволяет закрыть все риски, связанные с неавторизованным подключением к сети, с устаревшим антивирусного ПО, с наличием вредоносных программ, способных навредить сети. А также с наличием регламентов доступа, которые пользователи принимают и применяют в своей деятельности».
«NAC — это даже не технология, это идея, — считает Алексей Воронцов. — Она может быть реализована различными, зачастую несовместимыми друг с другом подходами».
— Идея NAC проста, — поясняет Михаил Орешин. — Необходимо получить информацию о любом подключаемом к сети устройстве, из любой точки и любым способом (через проводное, беспроводное подключение, канал VPN и пр.), и в автоматическом режиме принять решение по данному устройству или пользователю: разрешить ли ему доступ в корпоративную сеть компании, и если да, то с какими правами.

По мнению Орешина, более высокую управляемость всей сети обеспечивают не рекомендации, а принуждение. При этом контроль исполнения корпоративных политик будет эффективным, если есть удобный инструмент для их исполнения.
На рынке не существует продукта, где были бы реализованы все эти пять функций. Да и заказчики не торопятся внедрять весь комплекс мер по укреплению обороны корпоративной сети. Основная часть заказчиков пытается решить одну–две проблемы и чаще всего фокусируется на идентификации и разработке политик пользовательского доступа, а также на ликвидации угроз, которые проникают в сеть вместе с инфицированными хостами.
Наиболее полная реализация технологии NAC базируется на аппаратных средствах: специализированные устройства NAC позволяют тратить минимум усилий на внедрение технологий комплексной защиты доступа к сети и не зависеть ни от сетевого оборудования, которое используется в компании, ни от типа операционной системы.

Сценарии NAC
Константин Троицкий отмечает, что технология NAC изначально была запланирована для масштабного внедрения в крупной компании. Но в реальной жизни выбор того или иного решения NAC зависит в значительной степени от тех проблем, которые стоят перед заказчиком. Он должен четко понимать, какие риски закроет внедряемое решение NAC.

Алексей Воронцов, системный архитектор Центра информационной безопасности компании «Инфосистемы Джет», отмечает: «В отношении корпоративной сети очень высокая степень рисков связана с размещением компании во временном арендованном помещении, доступ в которое не контролируется сотрудниками самой компании. Повышенные риски представляют временные работники —

например, нанятые под какой-то проект. В таких случаях технология NAC особенно выгодна». Воронцов выделяет несколько сценариев для реализации технологии NAC.

1. Несоответствие корпоративным политикам безопасности (например, отставание обновлений ОС или баз антивируса) может возникнуть при возвращении сотрудника после кратковременного отсутствия на рабочем месте (командировка, отпуск, болезнь). При нарушении соответствия внутренним политикам сотрудник получает доступ к внутренней изолированной зоне сети (карантин), где ему предоставляется доступ к файловому ресурсу, с которого можно загрузить на компьютер новый антивирус, актуальные обновления и пр. Только после этого пользователю будет предоставлен полноценный доступ к сети и ее информационным ресурсам.
2. Офисная инфраструктура поддерживает функционирование двух сетей в компании — собственно офисной сети для внутренних сотрудников и зоны для гостевого доступа. Компания, открытая на рынке для общения с партнерами, заказчиками, может оказать гостеприимную услугу своим посетителям, предоставив им доступ в Интернет. Гость может просмотреть новости, свою корпоративную почту, без риска нарушения целостности внутреннего пространства сети. При этом гостю предлагается проверить — в том числе без агента — компьютер на предмет наличия антивирусов, и после проведения проверки (в случае ее успешного завершения) посетители, не являющиеся сотрудниками компании, направляются в защищенный сегмент с ограниченными правами доступа в Интернет.
3. Любой переезд офиса или филиала компании приводит к необходимости особенно внимательно отслеживать все подключения к сети.
4. Тем, кто по роду службы часто бывает в командировках, проживает в гостиницах, NAC обеспечивает удаленный доступ из этих мест к ресурсам по VPN с авторизацией на уровне сети и на уровне приложений.
5. Сменная работа персонала в многопользовательской среде требует идентификации сотрудников и отслеживания продолжительности их рабочего времени.
6. Решение для оператора связи. В сеть оператора вредоносный код поступает с зараженных компьютеров пользователей. Объединенные в ботнеты, такие компьютеры часто сами становятся источниками рассылки спама, не подозревая того. Но при наличии тарифных планов с неограниченным трафиком данная проблема существует уже не на уровне пользователей — она становится головной болью оператора связи. Технология NAC дает гарантию, что клиенты оператора подготовлены к прогулке в Паутине, и компьютер клиента не станет объектом для насаждения программ-дозвонщиков, изменяющих параметры сетевого соединения и подключающих компьютер пользователя к Интернету через каких-нибудь «гондурасских» провайдеров.

«Возможности NAC обширны, — говорит Алексей Воронцов. — Но основная часть работ по внедрению NAC, которые нам приходится выполнять даже сейчас, в кризисное время, представляет собой классические проекты для офисных систем».

NAC в гетерогенном окружении

Олег Головенко, системный инженер по продуктам безопасности Symantec

В последнее время компания Symantec несколько изменила свой взгляд на проблемы ИБ: если раньше основное внимание уделялось защите внутреннего периметра сети, то теперь фокусом информационной безопасности являются данные, где бы они ни находились — в корпоративной сети или на ноутбуке сотрудника. Основной продукт для обеспечения безопасности подключения пользователей к сети — Symantec Network Access Control (SNAC) — классический инструмент

обеспечения безопасности конечных точек, интегрированный с Symantec Endpoint Protection и обеспечивающий периодическое (по умолчанию каждые две минуты) сканирование конечных устройств на соответствие политикам безопасности.
В реализации Symantec NAC Symantec придерживается своего основного принципа — независимости от производителей сетевого оборудования и разработчиков ПО. Это означает, что продукт SNAC сможет работать в сетях и структурах с любым гетерогенным оборудованием. Это же касается и ПО на конечных точках: в SNAC включены проверки практически всех самых известных на сегодняшний день антивирусов, систем предотвращения вторжений, межсетевых экранов. Если малоизвестных вендоров нет в этом списке — их можно добавить вручную.
Среда принуждения в SNAC состоит из четырех основных компонентов, которые могут работать как автономно, так и в комплексе.
1.Symantec self enforcement
Самопринуждение — самый простой и дешевый подход, позволяющий применить технологию NAC без использования какого-либо дополнительного оборудования. Все ограничения действий пользователя происходят на конечной точке с помощью межсетевого экрана, который входит в состав Symantec Endpoint Protection. Помимо межсетевого экрана, задействуется и весь остальной функционал Symantec Endpoint Protection: система предотвращения вторжений, контроль приложений и устройств. Единственное, что остается сделать заказчику, — это приобрести сам Symantec Endpoint Protection. А SNAC будет действовать как его часть, выполняя функции и консоли управления, и агента на машине.
2 Шлюзовое решение Symantec Gateway Enforcer может использоваться при доступе по VPN или через Wi-Fi. Устройство ставится в разрыв между шлюзом и внутренней сетью.
3. Symantec DFCP Enforcer — устройство, устанавливаемое в разрыв между конечной точкой и сервером DFCP. Оно может ограничивать выдачу IP-адресов для конечных устройств. Есть вариант использования для Microsoft DFCP — сервера, если у заказчика развернута такая среда. В этом случае оборудование покупать не придется: достаточно установить ПО на сервер DFCP, и оно будет работать точно так же, как стандартный DFCP Enforcer.
4. Наиболее интересное решение — LAN Enforcer 802.1.x. Это устройство подключается к коммутаторам и позволяет открывать или блокировать порты коммутатора при попытке физического подключения к ним.
Без дополнительного устройства можно воспользоваться функциональностью продукта Symantec Endpoint Protection — определением местоположения конечной точки Location Awareness (IP-адрес, активная сетевая карта, MAC-адрес, доступность сервера DFCP, доступность других ресурсов). Комбинируя критерии, агент на конечной станции может определить, где находится конечная точка (в корпоративной сети, вне ее или подключилась по VPN). В зависимости от того, где находится конечное устройство, можно назначать различные политики межсетевого экрана.
Кроме того, в SNAC присутствует функционал автоматического исправления. При определенных условиях автоматически либо с уведомлением пользователя происходит исправление текущей ситуации на машине: скачиваются обновленные антивирусные базы, запускается сервис антивируса, Firewall, устанавливаются патчи. Пользователь может и не заметить, что его машина была не в порядке.
Еще одна полезная функция, реализованная в SNAC, — это предоставление гостевого доступа, которое реализуется посредством веб-портала. Если в сети присутствует Symantec Gateway Enforcer или Symantec DFCP Enforcer, то можно организовать гостевой доступ в сеть: при подключении по Wi-Fi и при запуске любого браузера гость попадает на веб-страницу, где ему предлагается скачать on-demand агент. После загрузки на машину он действует как постоянный агент: проводит проверки, соединяется с сервером и

сразу же имеет возможность отправить на сервер результат выполнения. Этот агент будет удален с машины автоматически при первой же перезагрузке.

Константин Троицкий, руководитель технического отдела компании «Поликом Про»
На сегодняшний день можно говорить о том, что предложения NAC от разных вендоров уже достаточно «повзрослели» для реального внедрения. Любая компания, внедряющая NAC, получает сразу ряд преимуществ, и в первую очередь повышение управляемости своей инфраструктуры, централизованный и унифицированный контроль защитных механизмов. Все это позволяет повысить уровень защиты от различных инцидентов безопасности, а многие — предотвратить, так как при нормально функционирующем NAC любые отклонения от «нормы» (установленной политикой безопасности компании или другими регламентами и требованиями) сразу же фиксируются и могут быть устранены. Однако, говоря о решении NAC сегодня, нельзя забывать о сложности самой поставленной задачи — а это унифицированный контроль самых разных политик. Решение NAC в подавляющем большинстве случаев не будет «вещью в себе», замкнутым и самодостаточным продуктом одного вендора в инфраструктуре компании: оно по своей природе строится на взаимодействии множества компонентов информационной системы, тесной интеграции самых разных программных и аппаратных продуктов. То есть решение NAC всегда будет включать в себя продукты разных вендоров, их интеграцию. На сегодняшний день вариант такого «решения из коробки», которое бы охватило все основные сферы и задачи сразу, выглядит нереалистичным. Но в дальнейшем как раз, на наш взгляд, развитие NAC будет направлено на унификацию базовых задач и интеграцию со все большим числом смежных продуктов.

Иллюстрация NAC
Решение любого производителя NAC функционирует на базе трех принципиальных компонентов. Во-первых, это точка, которая запрашивает доступ. Во-вторых, это сервер принятия решения. И в третьих, это среда принуждения, в которой реализуются установленные политики.
Рассмотрим один из сценариев функционирования NAC на примере Microsoft NAP. Ядро Microsoft NAP — это концепция «Сертификации о здоровье», Health Certification. Конструированием этого сертификата, выдаваемого на основании состояния машины, занимается специальный агент, взаимодействующий с антивирусами, программами обнаружения шпионов, персональными межсетевыми экранами. Разработчики этого программного обеспечения занимаются также написанием связующих компонентов, которые позволяют объединять их продукты со специальным агентом Microsoft.
В рамках функционирования NAP клиент пытается подключиться к коммутатору с поддержкой 802.1 на портах. Как только происходит аутентификация 802.1x, специальный агент отправляет «Сертификат о Здоровье» на центральный узел принятия решения — системный сервер System Health Server. Это устройство на основании информации о состоянии машины принимает решение и передает информацию на сервер сетевых политик — Microsoft Network Politic Server, NPS. В свою очередь NPS взаимодействует с коммутатором 802.1x, обеспечивая VLAN для доступа, для карантина либо для ликвидации угроз.

Два подхода

При всем многообразии продуктов можно выделить два основных подхода вендоров к построению архитектуры NAC. Первый подход, представителями которого являются Microsoft и Cisco, состоит в подготовке конструктора, набора инструментов для автоматизации и реализации технологий планирования. В состав конструктора Cisco NAC Framework входит сервер сетевых политик Network Policy Server, называемый Access Control System (ACS), а также оборудование и специализированное ПО Cisco. Для того чтобы выдать сертификат, подтверждающий лояльность подключаемой к сети машины, специализированный агент должен взаимодействовать с множеством продуктов партнеров: например, Cisco NAC работает с Trend Micro, MacAfee, а также продуктами «Лаборатории Касперского».

Второй метод состоит в том, что разработчик NAC самостоятельно предоставляет поддержку сторонних компонентов — антивирусного или антишпионского ПО. Такого подхода придерживается, например, компания Symantec, которая централизованно разрабатывает эту поддержку. Благодаря тому что за написание соответствующего плагина для NAC отвечает сама компания Symantec, как разработчик антивирусного решения, это позволяет избежать отставания — например, зазора между выходом новой версии антивируса и поддержкой проверки этого антивируса в продукте NAC, не говоря уж об обновлении продукта.

Присутствующие на рынке решения отличаются гибкими настройками и наличием средств централизованного управления. Требования задаются свободно в форме сценариев, выполнена частичная интеграция с различными инфраструктурными средствами (антивирусы, обновления, домены, PKI). Для присутствующих на рынке решений характерно наличие развитых механизмов отчетности и оповещения, реакции на инциденты.

Непрерывная оценка состояния конечных точек вкупе с идентификацией формирует основу для эффективной реализации NAC. Большое значение имеет легкость развертывания и простота эксплуатации таких продуктов. Идентификация (например, возможность на ее основе отклонить доступ) — одна из основных функций NAC. Эффективное решение NAC не должно добавлять дополнительных точек отказа или узких мест в сетевой инфраструктуре. Оценка конечной точки и разработка политик ведутся на уровне конечной точки, а принуждение, непрекращающийся сетевой анализ и оценка ресурсов — это работа на уровне сетевой инфраструктуры.

Вендоры предпочитают предлагать в рамках своих решений NAC либо хорошо реализованные функции оценки состояния конечных точек, карантин, процесс корректировки и непрекращающийся анализ угроз, либо политику принуждения на основе идентификации. Но обе возможности вместе никто не предлагает.

Будущее NAC

— В будущем решение NAC должно обеспечивать полную интеграцию с различными сторонними решениями — например, с системами обновления, — считает Константин Троицкий. — В дальнейшем развитие этих решений, скорее всего, будет идти по пути интеграции с такими крупными платформами по управлению инфраструктурой, как IBM Tivoli, HP OpenVew, Microsoft Configuration Manager или Altiris. Кроме того, неизбежна интеграция этих решений с системами автоматического определения типа клиентов, системами проактивного мониторинга, системами IDS/IPS, а также системами предотвращения утечек, Data Leakage Protection. Наряду с этим, появится поддержка новых клиентских устройств.

В дальнейшем все решения NAC станут поддерживать универсальный динамический гостевой доступ, а решения NAC «из коробки» будут обеспечивать минимальные затраты

на обновление и внедрение.

«Пользователю неинтересно хранить множество идентификационных атрибутов и каждый раз предъявлять их при доступе в здание или помещение, при загрузке рабочей станции, при подключении к сети, регистрации в домене, доступе к сетевым ресурсам, — говорит Виталий Томилко. — В идеале решения NAC будут интегрироваться с системами однократной аутентификации и авторизации Single Sign-On на основе цифрового сертификата и его носителя (USB-токена с интегрированной RFID-меткой)». По мнению Виталия Томилко, будущее этих систем связано с тенденцией виртуализации как серверных ресурсов, так и настольных систем. Все приложения будут выполняться в виртуальной среде, и рабочая станция превратится в тонкий клиент, подключаемый к ресурсам крупного центра обработки данных. В этом случае продукты NAC развернутся в таком виртуальном облаке; с их помощью будет обеспечиваться безопасность виртуальных десктопов, так что сложность решений только увеличится.