Основы NAC-систем

Введение

Все устройства, подключаемые к корпоративной или частной сети, потенциально несут риск для организации. Если на устройстве отсутствуют важные обновления операционной системы или антивирусного ПО, или есть предположение, что оно заражено вредоносным ПО, то разрешение доступа означает предоставление злоумышленнику инструментов доступа к сети. Для снижения вероятности таких рисков были разработаны программные решения класса NAC (далее, NAC-системы).

NAC (англ. Network Access Control) — это тип программного решения в области безопасности, которое контролирует, кто может получить доступ к сети и в каком объеме. Такого типа решения обеспечивают прозрачность в сети и позволяют управлять доступом путем применения на подключаемых к сети устройствах политик безопасности.

Основные возможности NAC-систем:

- **Видимость устройств и профилирование:** NAC предоставляет организациям возможность видеть, какие устройства подключаются к сети, и возможность профилирования этих устройств и их пользователей;
- **Проверка защищённости сети:** NAC-системы разрабатываются с расчетом, что только авторизованные и соответствующие политикам устройства могут получить доступ к корпоративной сети и ее ресурсам;
- **Ограничение доступа к сети:** NAC может полностью заблокировать неавторизованные или не соответствующие политикам устройства или предоставить им ограниченный доступ к корпоративным ресурсам. Это позволяет организациям предоставлять ограниченный доступ гостевым пользователям, партнерам, неавторизованным или несущим риск устройствам;
- **Управление политиками безопасности:** NAC позволяет организациям централизованно управлять политиками безопасности и применять их на конечных точках. Это позволяет организациям более просто обновлять политики безопасности для конечных точек для того, чтобы учитывать возрастающие риски или ужесточающиеся требования соответствия.

Все NAC-системы можно разделить на два основных типа:

- **Решения, которые выполняют проверку перед предоставлением доступа (pre-admission):** ограничивают доступ к сети полностью. Прежде чем устройству будет предоставлен какой-либо доступ к сети, оно проверяется на соответствие политикам безопасности и соответствующие права;
- **Выполняют проверку после предоставления доступа (post-admission):** разрабатываются с целью предотвратить перемещение злоумышленника по сети. Если пользователь или устройство пытаются получить доступ в другом сегменте сети, они проверяются на наличие прав и соответствие политикам безопасности повторно.

В настоящее время NAC-системы используются в следующих целях:

- **AAA:** NAC выполняет процессы авторизации, аутентификации и аккаунтинга всех подключаемых к сети устройств на порте. Таким образом, ни одно чужое устройство ну сможет попасть в защищенную сеть.
- **Профилирование:** NAC позволяет определять модели оконечных устройств, их операционную систему, производителя, месторасположение, тем самым применяя определенный профиль на устройство. Благодаря профилированию, устройство, которое сменило систему или, например, местоположение может быть помещено в карантин для дальнейшей проверки.
- **BYOD:** NAC позволяет пользователю самостоятельно добавить личное устройство и обеспечить его безопасность. Система гарантирует, что подключаемые удаленно устройства соответствуют корпоративным политикам безопасности, перед тем как им будет предоставлен доступ к сети;
- **IoT:** NAC может ограничивать доступ устройствам такого типа к корпоративной сети, в виду их значительной угрозы для безопасности (являются частыми объектами атак киберпреступников);
- **Гостевой/ролевой доступ:** Данная группа пользователей может иметь законные потребности в получении сетевого доступа, однако им не требуется получать полный доступ. NAC может применять ограничения, исходя из роли пользователя;
- **Изоляция зараженных устройств:** Вредоносное ПО может пытаться распространиться по сети. NAC-системы могут заблокировать их путем перемещения потенциально зараженных устройств в карантин.

Обобщим вышеизложенное — основной задачей NAC-систем является обеспечение видимости и контроля за использованием сети. Т.е. NAC-система позволяет видеть, кто пытается получить доступ к сети, а в случае с NAC, выполняющими проверку после предоставления доступа (post-admission NAC), видеть, каким образом устройство ведет себя в сети и применять ограничения в случае, когда устройство ведет себя подозрительно.

Методы аутентификации

Все устройства, которые подключаются к защищенной сети должны проходить процесс аутентификации на порту коммутатора/контроллере Wi-Fi.

Существует три основных метода аутентификации:

- **IEEE 802.1x:** аутентификация по стандарту 802.1x;
- **MAC Authentication Bypass (MAB):** аутентификация по MAC-адресу устройства (применяется для устройств, которые не поддерживают 802.1x);
- **Web Authentication:** аутентификация посредством ввода связки логина и пароля в веб-портале (может использоваться как дополнительный метод защиты).

Аутентификация по стандарту IEEE 802.1x

IEEE 802.1X — это стандарт IEEE для управления сетевым доступом с аутентификацией на портах (PNAC), который входит в группу сетевых протоколов IEEE 802.1. Он обеспечивает механизм аутентификации для устройств, желающих подключиться к локальной или беспроводной сети. Данный стандарт описывает процесс инкапсуляции данных **Расширяемого Протокола Аутентификации (EAP)**, передаваемых между запрашивающими устройствами (клиентами), системами, проверяющими подлинность (коммутаторами, точками беспроводного доступа), и серверами проверки подлинности (RADIUS).

Таблица 1 — Основные термины

Клиент/Супликант	Программное обеспечение на конечной стороне (также называемое **пир (peer)**), которое взаимодействует с EAP второго уровня. Данное ПО отвечает аутентификатору и предоставляет идентификационные данные.
Аутентификатор/NAS	Сетевое устройство, которое управляет физическим доступом к сети на основе статуса аутентификации конечной точки. Аутентификатор выступает в качестве посредника, принимающего сообщения EAP второго уровня от супликанта и инкапсулирующего их в RADIUS, направленные на активный сервер аутентификации. Наиболее распространенными аутентификаторами являются коммутаторы и контроллеры беспроводных сетей (WLC).
Сервер аутентификации	Сервер, выполняющий фактическую аутентификацию клиента. Он проверяет идентификационные данные конечной точки и предоставляет аутентификатору результат, например согласие или отказ.
Источник идентификации	Список устройств или пользователей, который может быть как внутри сервера аутентификации, так и снаружи.

Аутентификация клиента происходит в несколько этапов:

1. **Инициализация:** На этом этапе клиент подключается к порту аутентификатора. Аутентификатор распознает факт подключения и активизирует логический порт для клиента, сразу переводя его в состояние "неавторизован" (uncontrolled). В результате через клиентский порт возможен лишь обмен трафиком протокола 802.1x, для всего остального трафика порт заблокирован.
2. **Инициация:** Аутентификатор ожидает от клиента запрос на аутентификацию (EAPOL-Start). Когда аутентификатор получает запрос, он посылает клиенту EAP-request/identity. Клиент в ответ высылает EAP-response со своим идентификатором (например, именем пользователя), который аутентификатор перенаправляет в сторону сервера аутентификации, предварительно завернув в RADIUS Access-Request.
3. **Обмен EAP:** Сервер аутентификации и клиент договариваются о методе EAP, по которому будет проходить аутентификация.
4. **Аутентификация:** Может происходить по-разному, в зависимости от метода EAP. В результате сервер аутентификации разрешает (accept) или запрещает (reject) доступ, с пересылкой данного сообщения аутентификатору. В случае успешной аутентификации аутентификатор переводит порт клиента в состояние «авторизован» (controlled), и начинается передача трафика клиента.

Методы EAP

EAP – протокол, который стандарт 802.1x использует для управления взаимными аутентификациями. Обладая

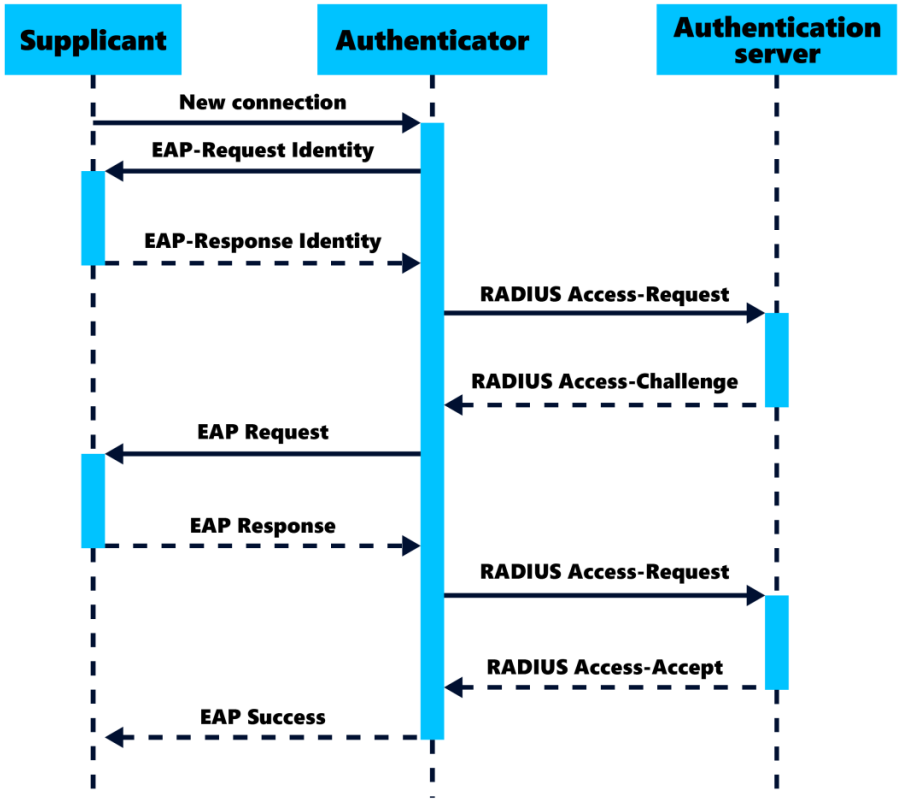
стандартизированным протоколом EAP, клиенту совершенно не требуется вникать в тонкости методов аутентификации. Аутентификатор просто работает посредником, формируя и распаковывая EAP-пакеты, чтобы направить их от запрашивающего на сервер аутентификации, где, собственно, и будет происходить сам процесс аутентификации. В настоящее время определено около 40 различных методов EAP-аутентификаций, но мы рассмотрим самые основные.

EAP-MD5

Метод EAP-MD5 использует алгоритм дайджеста сообщений для скрытия учетных данных в хэш. Хэш отправляется на сервер, где он сравнивается с локальным хэшем, чтобы проверить, совпадают ли идентификационные данные. Однако EAP-MD5 не имеет механизма взаимной аутентификации. Это означает, что сервер проверяет клиента, но клиент не аутентифицирует сервер (то есть не проверяет, следует ли ему доверять серверу). Чаще всего такой метод используется для аутентификации IP-телефонов.

Алгоритм работы:

1. Сервер аутентификации посылает запрос EAP-Request-Identity клиенту.
2. Клиент в ответ посылает EAP-Response-Identity.
3. После получения EAP-Response-Identity сервер генерирует случайную строку (challenge string) и отправляет клиенту MD5-Challenge-Request с этой строкой.
4. Клиент объединяет имя пользователя, пароль в открытом виде и challenge string в одно значение и отправляет хэш MD5 этого значения на сервер аутентификации как MD5-ChallengeResponse
5. После получения MD5-Challenge-Response сервер аутентификации самостоятельно считает MD5-хэш от данных пользователя и отправленной строки challenge string и сравнивает с хэшем, полученным от клиента. Если хэши совпадают, аутентификация завершается успешно.



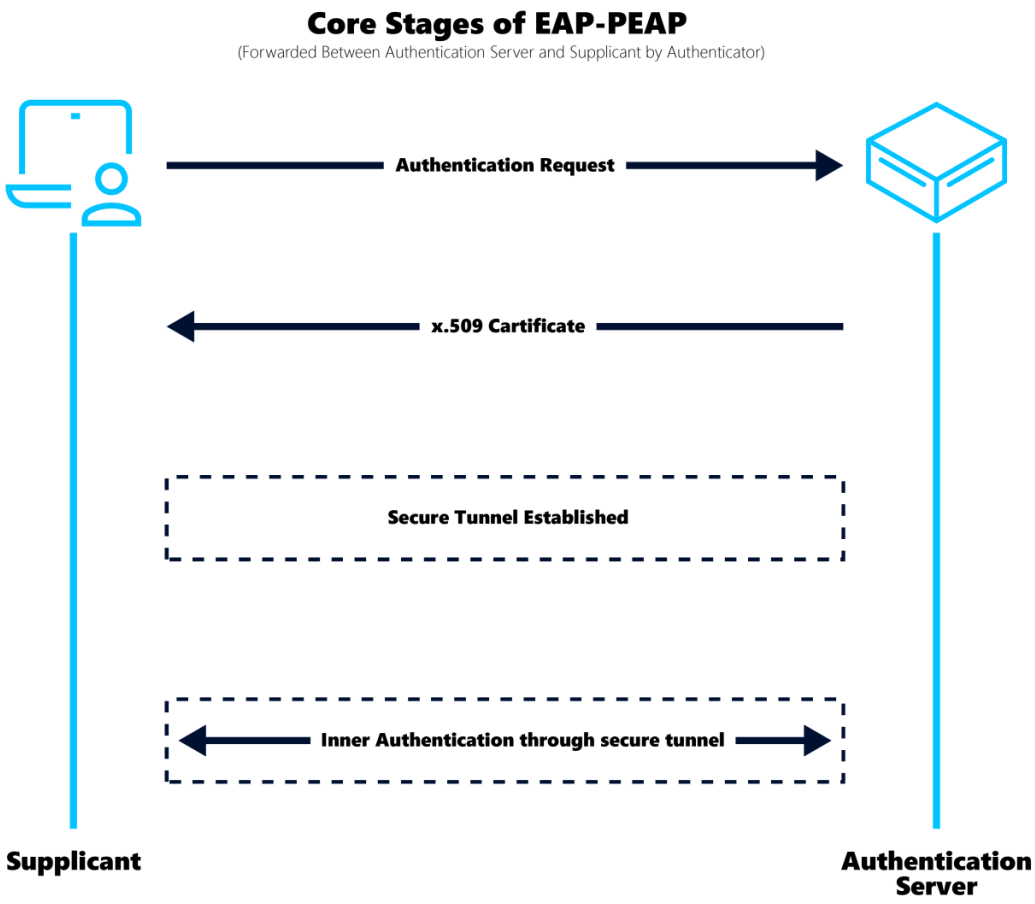
PEAP

PEAP (Protected EAP/PEAP) — метод, первоначально предложенный компанией Microsoft. Он представляет собой тип туннеля EAP, который быстро стал самым популярным и широко распространенным методом EAP в мире. PEAP формирует потенциально зашифрованный TLS-туннель между клиентом и сервером, используя сертификат x.509 на сервере, точно так же, как SSL-туннель создается между веб-браузером и защищенным веб-сайтом. После того как туннель сформирован, PEAP использует какой-либо другой метод EAP в качестве "внутреннего метода", аутентифицируя клиента с помощью EAP внутри внешнего туннеля.

Алгоритм работы:

Аутентификация проходит в 2 этапа – внешний и внутренний.

1. Внешняя аутентификация:
    a. Клиент посылает Authentication Request на сервер аутентификации.
    b. Сервер в ответ посылает свой сертификат
    c. Клиент проверяет сертификат сервера, и, если всё в порядке, внешняя аутентификация проходит успешно.
    d. Клиент и сервер устанавливают TLS-соединение.
2. Внутренняя аутентификация через установленный безопасный канал. При этом существует много различных протоколов аутентификации, однако наиболее часто используется MS-CHAPv2.



EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) — это протокол EAP, который расширяет TLS. Клиент может, но не обязан проходить аутентификацию с помощью сертификата подписанного на сервере. Это значительно упрощает процедуру настройки, поскольку сертификат не требуется каждому клиенту. После того как сервер аутентифицирован для клиента с помощью сертификата и, по желанию, клиент для сервера, сервер может использовать установленное безопасное соединение ("туннель") для аутентификации клиента. Он может использовать существующий и широко развернутый протокол аутентификации и инфраструктуру, включающую устаревшие механизмы паролей и базы данных аутентификации, а защищенный туннель обеспечивает защиту от перехвата и атак типа "человек посередине". В таком методе имя пользователя никогда не передается открытым текстом без шифрования, что повышает безопасность.

Алгоритм работы идентичен предыдущему методу.

EAP-TLS

EAP-TLS — метод, использующий TLS для обеспечения безопасной передачи идентификационных данных. Преимущество данного метода в том, что он является открытым стандартом IETF и поддерживается почти всеми устройствами. EAP-TLS использует сертификаты X.509 и обеспечивает возможность поддержки взаимной аутентификации, при которой клиент проверяет сертификат сервера, и наоборот. Он считается одним из самых безопасных методов EAP, поскольку перехват пароля невозможен. При этом, конечная точка все равно должна иметь закрытый ключ.

Алгоритм работы в данном методе схож с двумя предыдущими. Главное отличие заключается в том, что на внешнем этапе аутентификации происходит проверка подлинности не только сервера, но и клиента. После взаимной проверки подлинности аутентификация проходит по протоколу TLS.

Внутренние методы

Также существуют внутренние методы EAP. Они выделены в отдельную категорию, так как они используются только

внутри других методов, например, PEAP и EAP-TTLS:

- **PEAP-MSCHAPv2** — при использовании этого внутреннего метода идентификационные данные клиента отправляются на сервер в зашифрованном виде в рамках сессии MSCHAPv2. Это наиболее распространенный внутренний метод, поскольку он позволяет просто передавать имя пользователя и пароль или даже имя компьютера и пароль компьютера на RADIUS-сервер, который, в свою очередь, проверяет их подлинность в Active Directory.
- **EAP-GTC** — этот внутренний метод был создан компанией Cisco в качестве альтернативы MSCHAPv2 и позволяет выполнять стандартную аутентификацию практически в любом хранилище идентификационных данных, включая серверы токенов OTP, LDAP, Novell E-Directory и т.д.
- **EAP-TLS** — PEAP и EAP-TTLS способны использовать EAP-TLS в качестве внутреннего метода.

RADIUS

Протокол RADIUS является IETF-стандартом для аутентификации, авторизации и аккаунтинга. Сведения от аутентификации и авторизации доставляются одним типом пакетов, а аккаунтинг обрабатывается отдельным процессом. Современная реализация RADIUS использует порты 1812 (аутентификация) и 1813 (аккаунтинг) протокола UDP (также возможно использование портов 1645 и 1646). UDP обладает высокой скоростью, но имеет ряд недостатков, которые необходимо учитывать при его применении. Когда разрабатывали RADIUS, вопросы безопасности не были столь актуальны, как сейчас, поэтому он поддерживает довольно малое число типов аутентификации (Clear text и CHAP), шифрует только поле с паролем и в целом имеет среднюю степень безопасности. В NAC-системах используется как транспорт от коммутатора/WLC до сервера сервера аутентификации.

Рассмотрим основные типы RADIUS-сообщений, используемых в NAC-системах:

Access-Request

Это сообщение отправляется от клиента к серверу аутентификации для запроса аутентификации и/или авторизации. Запрашиваемая функция называется типом службы. Например, для аутентификации по стандарту IEEE 802.1x значением типа сервиса будет **"framed"**.

Access-Accept

Данное сообщение отправляется от сервера аутентификации клиенту, сообщая о прохождении аутентификации.

Access-Reject

Данное сообщение отправляется от сервера аутентификации клиенту, сообщая об отклонении аутентификации.

Access-Challenge

Данное сообщение опционально. Оно может быть отправлено от сервера аутентификации, когда необходима дополнительная информация, например, код для двухфакторной аутентификации. Также такое сообщение отправляется при необходимости продолжения взаимодействия. Например, при аутентификации по протоколу EAP-TLS, для построения сессии, будет отправлено несколько сообщений Access-Challenge.

Accounting-Request

Данное сообщение отправляется от клиента к серверу аутентификации для запроса сервиса обработки аккаунтинга. Оно может включать в себя информацию о времени, пакетах, DHCP, CDP и т.д. Такое сообщение может содержать два параметра — **START** для сообщения о начале работы сервиса и **STOP** для сообщения о конце его работы.

Accounting-Response

Данное сообщение отправляется от сервера аутентификации к клиенту и является подтверждением получения сообщения **Accounting-Request**.

Аутентификация по MAC-адресу (MAC Authentication Bypass)

MAC-аутентификация — метод аутентификации, который предоставляет доступ в сеть, аутентифицируя конкретное устройство, а не пользователя. Когда устройство подключается к коммутатору (непосредственно или через другой коммутатор), коммутатор отправляет MAC-адрес устройства на RADIUS-сервер для прохождения аутентификации.

Коммутатор отправляет на RADIUS-сервер, вместо имени пользователя и пароля, MAC-адрес устройства. Соответственно в базу данных пользователей (источник идентификации) должна быть добавлена запись пользователя с именем — MAC-адрес устройства и паролем — MAC-адрес устройства.

От клиента в таком случае не требуется никаких действий и на устройстве не нужны никакие дополнительные настройки. Коммутатор сам запоминает MAC-адрес и отправляет запрос на RADIUS-сервер.

MAC-аутентификация может применяться для устройств, которые не поддерживают протокол 802.1x (принтер, сервер, камера видеонаблюдения и т.д.).

Web-аутентификация

Web-аутентификация — метод аутентификации, который предоставляет доступ в сеть аутентифицируя пользователя через веб-интерфейс. Не требует установки дополнительного программного обеспечения, для аутентификации клиенту нужен только браузер.

Если на порту включена Web-аутентификация, то клиент не может использовать прокси-сервер в браузере.

ID статьи: 7
Последнее обновление: 30 окт., 2025
Обновлено от: Ильина В.
Ревизия: 16
База знаний AxelNAC -> Обучающие материалы -> Основы NAC-систем
https://docs.axel.pro/entry/7/