

Как защитить удалённое подключение к ресурсам организации с помощью MFA-решения NetIQ Advanced Authentication

Многофакторная аутентификация (MFA, МФА) — один из надёжнейших способов проверки личности сотрудников, подключающихся к ресурсам организации. Проанализируем, как с помощью решения NetIQ Advanced Authentication реализовать дополнительные факторы аутентификации и устранить риски использования банальной связки «логин-пароль».

Оглавление

Введение	1
Архитектура решения	2
Методы и цепочки методов дополнительной аутентификации	5
События аутентификации	7
Защита подключения к виртуальным рабочим местам	8
Защита подключения к VPN	10
Использование многофакторной аутентификации для тонкой настройки доступа к ресурсам	11
Индивидуализация решения посредством API и SDK	12
Готовые интеграции с IAM-продуктами NetIQ от Micro Focus	12
Интеграция с риск-сервисом от Micro Focus	13
Выводы	14

Введение

Корпорация Micro Focus, являясь известным и значимым разработчиком программного обеспечения, имеет в своём портфеле множество разнообразных продуктов. Активно прогрессируют, в частности, решения по информационной безопасности, объединённые под названием «Security, Risk and Governance». Внутри этого подразделения существует относительно обособленная линейка решений по управлению учётными записями и доступом — Identity and Access Management (IAM), выступающая под общим брендом «NetIQ» (по названию компании, которая развивала эти продукты до поглощения

компанией Micro Focus). Мы хотим рассказать об одном из наиболее актуальных сегодня представителей этой линейки — программном средстве многофакторной аутентификации NetIQ Advanced Authentication.

Актуальность данного продукта многократно возросла именно сейчас в связи с ужесточением карантинных мер по всему миру и вызванным ими повсеместным переводом работы в удалённый режим. Раньше, во времена «офисной жизни», при доступе пользователя к ресурсам в основном было достаточно удостоверить его личность обычной парой «логин-пароль». Сегодня же, когда доступ запрашивается не изнутри периметра организации, а кем-то извне, кто знает упомянутую пару, доверие к этому фактору как единственному становится очень рискованным. Решения по многофакторной аутентификации призваны устранить данный риск за счёт дополнительной проверки подлинности пользователя. Чтобы подтвердить, что он действительно является тем, за кого себя выдаёт, сотрудник должен будет задействовать — в зависимости от решения и его настроек — дополнительные знания (ответы на контрольные вопросы, PIN-код), принадлежащее только ему оборудование (например, смартфон для отправки одноразового пароля, персональный аппаратный токен) или биометрические данные (отпечаток пальца, лицо и прочее).

Архитектура решения

Важной отличительной особенностью NetIQ Advanced Authentication является его высокий уровень масштабируемости, который опирается на встроенные средства обеспечения бесперебойной работы. Решение состоит из ряда архитектурных компонентов, которые можно распределить по разным серверам в зависимости от размера внедрения и требований к отказоустойчивости.

В простейшем случае NetIQ Advanced Authentication может быть развёрнут на единственном сервере, подключённом к LDAP-совместимому каталогу (например, Active Directory или eDirectory) и так называемому конечному устройству (Endpoint). Под последним подразумевается физическое или виртуальное устройство, на котором у пользователя будет запрашиваться дополнительная аутентификация. В качестве конечного устройства могут выступать рабочая станция под управлением Windows, macOS или Linux, сервер, окно аутентификации приложения, определённый URL, открытый в веб-браузере, и другие сущности. Схема этой архитектуры показана на рис. 1 и по очевидным причинам используется только для тестовых целей.

Рисунок 1. Схема простой архитектуры NetIQ Advanced Authentication



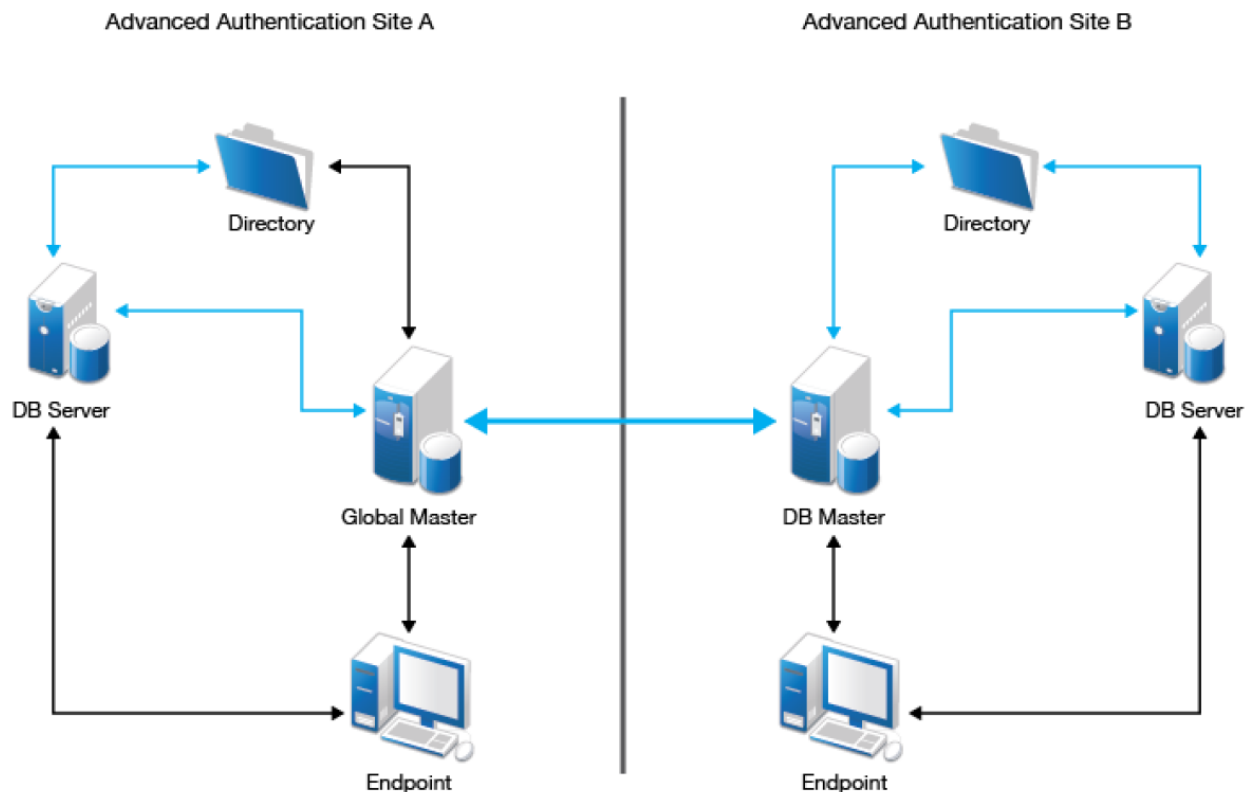
В реальных инсталляциях требования к отказоустойчивости сервиса предполагают дублирование компонентов на различных серверах, в том числе на различных площадках. В этом случае серверные компоненты NetIQ Advanced Authentication получают различные роли:

- **Global Master.** Роль главного сервера на весь кластер, содержащий базу данных NetIQ Advanced Authentication. Также сервер с этой ролью является регистратором новых серверов и площадок NetIQ Advanced Authentication.

- **DB Master.** Роль сервера БД, являющегося главным на данной площадке. На этот сервер осуществляется репликация БД с Global Master при инсталляции NetIQ Advanced Authentication на нескольких площадках.

- **DB Server.** Роль «рядового» сервера БД NetIQ Advanced Authentication. Используется как резервный на случай временной недоступности Global Master. После восстановления доступа информация синхронизируется и Global Master снова становится главным объектом взаимодействия с конечными точками NetIQ Advanced Authentication. Кроме того, DB Server удобно использовать для регулярного резервного копирования БД, освободив от этой нагрузки основной сервер.

Рисунок 2. Схема отказоустойчивой архитектуры NetIQ Advanced Authentication

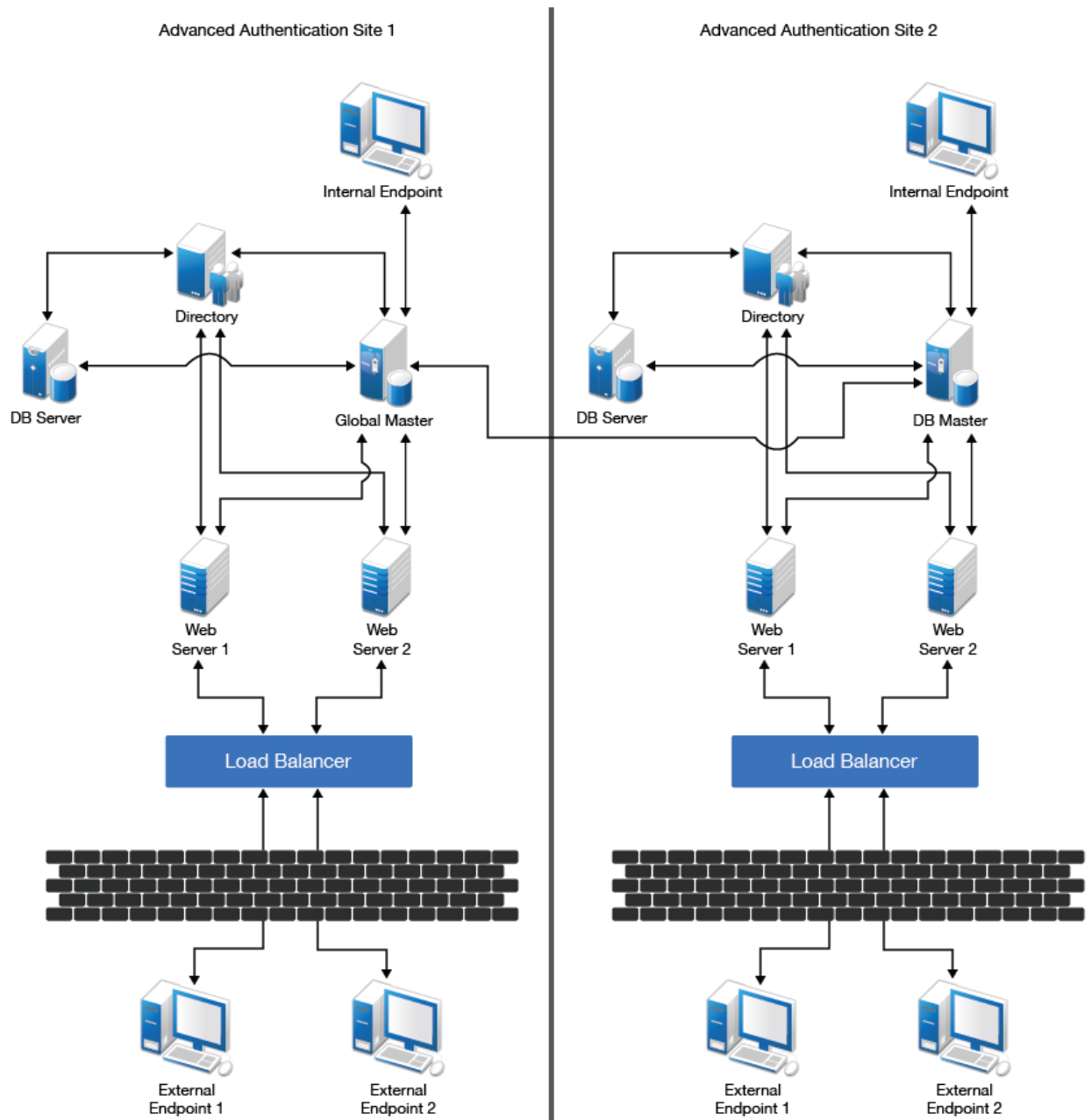


Для высоконагруженных сред NetIQ Advanced Authentication предлагает архитектуру с дополнительными компонентами: веб-серверами и балансировщиками нагрузки.

Веб-сервер не содержит БД NetIQ Advanced Authentication. Он используется для обработки запросов на аутентификацию и взаимодействует с базой данных Global Master (или DB Master). Есть возможность устанавливать дополнительные веб-серверы по мере роста количества одновременных запросов на аутентификацию в организации.

Балансировщик нагрузки используется для распределения запросов на аутентификацию со стороны внешних конечных устройств.

Рисунок 3. Схема отказоустойчивой архитектуры NetIQ Advanced Authentication с использованием балансировщика нагрузки



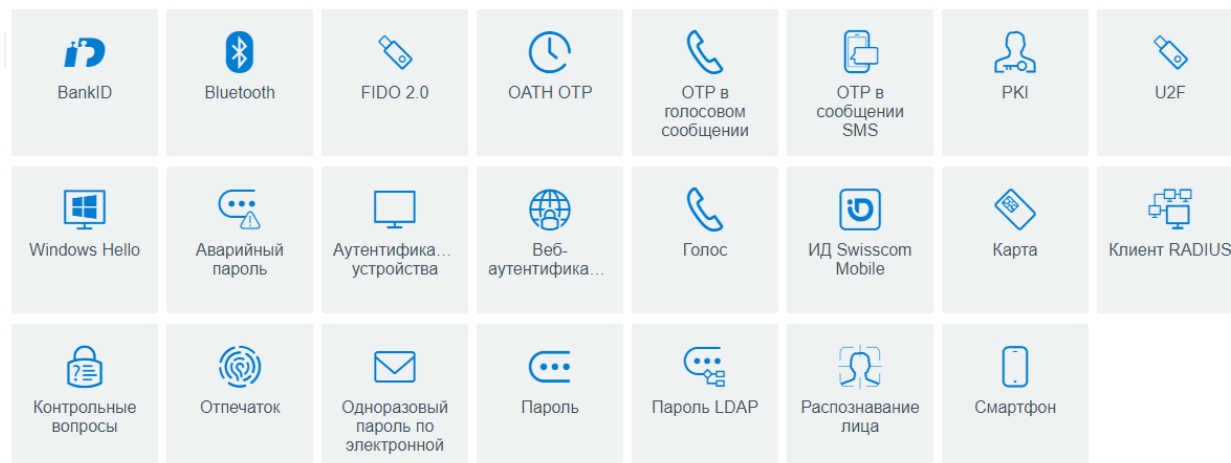
Методы и цепочки методов дополнительной аутентификации

Продукт NetIQ Advanced Authentication изначально разрабатывался как универсальное решение по многофакторной аутентификации, которым легко можно охватить самые сложные и нестандартные требования по безопасности. Поэтому в него была заложена поддержка разнообразных методов дополнительной проверки подлинности

пользователей. В настоящее время «из коробки» продукт поддерживает 23 метода аутентификации.

Рисунок 4. Поддерживаемые методы аутентификации в NetIQ Advanced Authentication


Методы



Любой из этих методов можно использовать как по отдельности, так и совместно с другими. При совместном применении методы аутентификации образуют т. н. «цепочки» (chains). Для обеспечения максимальной гибкости можно создавать различные комбинации для конкретных сценариев доступа и групп пользователей; в последнем случае настройка будет автоматически распространяться на всех новых участников этой группы. Такой подход позволяет сократить административные затраты в крупных организациях, а также снизить уровень риска, связанного с потенциальным отсутствием обязательной проверки подлинности для новых сотрудников.

Рисунок 5. Настройка цепочек методов аутентификации в NetIQ Advanced Authentication

Имя


Изображение  [Изменить...](#)

Включено ON

Методы

Available	Used
Bluetooth	Пароль LDAP
Карта	TOTP
Аутентификация устройства	Распознавание лица
Одноразовый пароль по электронной почте	
Аварийный пароль	
FIDO 2.0	

Репозитории, роли и группы

 MFVAAF_USERS

События аутентификации

Как говорилось выше, в NetIQ Advanced Authentication можно гибко настроить одну или несколько цепочек методов для различных сценариев доступа. Это делается через т. н. «события аутентификации» (events), в момент наступления которых пользователь видит окно с запросом дополнительных факторов аутентификации. В качестве примеров подобных событий в NetIQ Advanced Authentication можно привести следующие:

- вход в операционную систему (Windows, Linux, macOS);
- вход в мейнфрейм;
- подключение к VPN;
- доступ к приложениям и облачным сервисам через протоколы OAuth 2.0 и SAML 2.0;
- доступ к portalу самообслуживания для пользователей;
- доступ к веб-ресурсам через интеграцию с NetIQ Access Manager;
- доступ в ADFS.

Есть также возможность создать индивидуализированное событие аутентификации для интеграции NetIQ Advanced Authentication с нестандартными системами и приложениями.

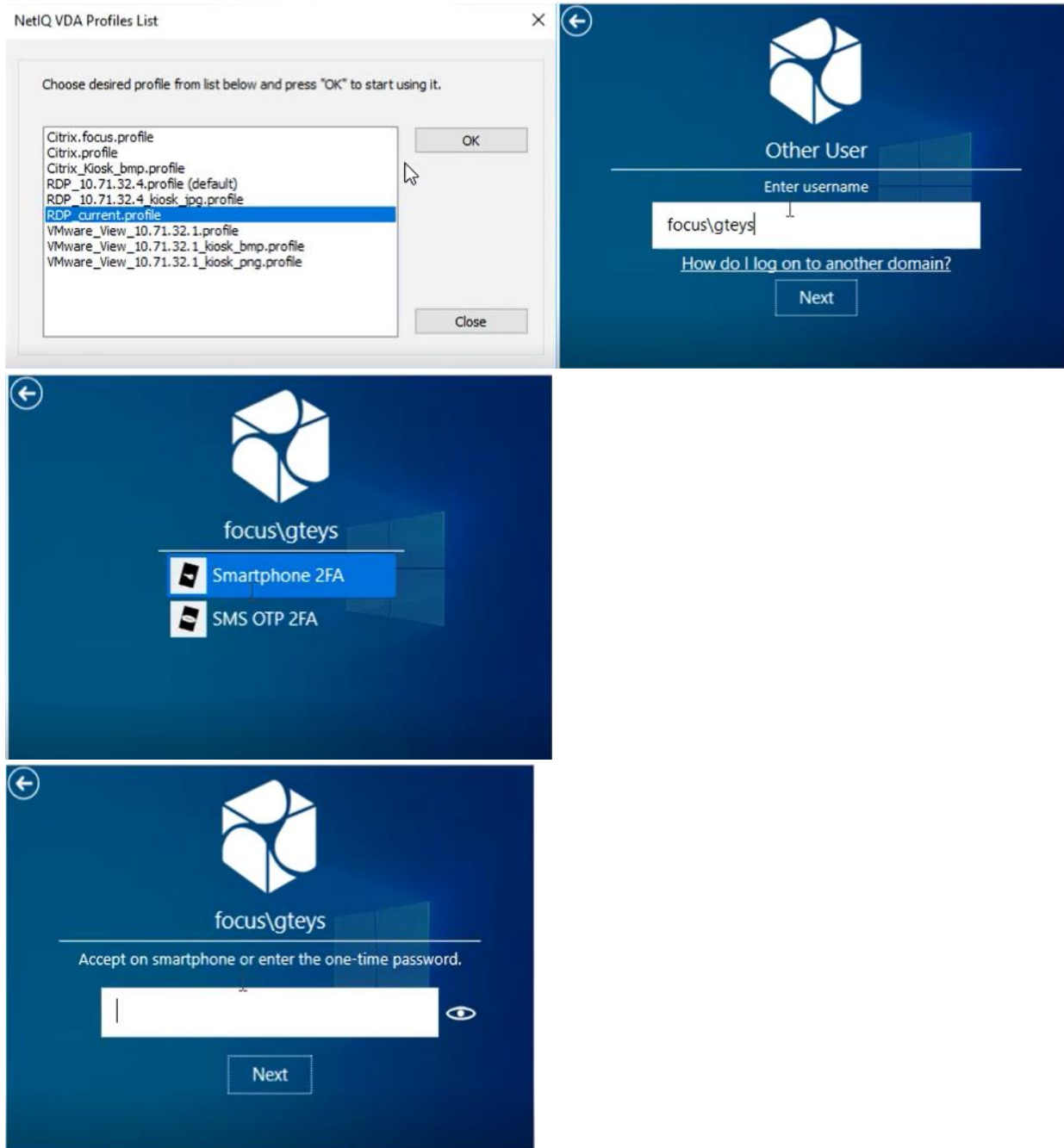
Далее рассмотрим применение NetIQ Advanced Authentication для реализации типовых сценариев защищённого удалённого доступа в организациях.

Защита подключения к виртуальным рабочим местам

NetIQ Advanced Authentication позволяет защитить подключение к инфраструктуре виртуальных рабочих столов (VDI). Для этого используется компонент Virtual Desktop Authentication Agent (VDA), который устанавливается на компьютер пользователя.

В качестве платформ виртуализации поддерживаются Citrix, VMware Horizon (ранее известный как VMware View) и Microsoft RDS. Работа агента VDA с тем или иным VDI-решением настраивается через профиль VDA. После того как всё будет настроено, при попытке подключиться к виртуальной рабочей станции пользователь сначала должен будет ввести дополнительные аутентификационные данные, запрашиваемые NetIQ Advanced Authentication. Примеры интерфейса показаны на рисунках.

Рисунки 6-9. Интерфейс NetIQ Advanced Authentication при подключении к виртуальной рабочей станции



Вышеописанный способ относится к предсессионной аутентификации, т. е. удалённая сессия открывается после прохождения проверки подлинности. Однако кроме такого варианта в NetIQ Advanced Authentication поддерживается и постсессионная аутентификация — например, если необходимо защитить не всю сессию, а только вход в определённые опубликованные приложения внутри неё. В этом случае компонент NetIQ Advanced Authentication под названием Device Service позволяет «пробросить» устройство дополнительной аутентификации (скажем, считыватель смарт-карты или сканер отпечатка

пальца) внутрь удалённой сессии. Таким образом достигается существенная гибкость при настройке защищённого удалённого подключения.

Защита подключения к VPN

Для обеспечения проверки подлинности пользователя при VPN-подключении используется RADIUS-сервер, встроенный в NetIQ Advanced Authentication. Сервер VPN в этом случае будет являться клиентом RADIUS и транслировать запросы VPN-клиента на сервер NetIQ Advanced Authentication. Далее MFA-решение будет проводить аутентификацию в соответствии с настроенными для данного события цепочками методов, а затем через сервер VPN взаимодействовать с пользователем для получения дополнительных аутентификационных данных.

Рисунки 10-13. Пример применения NetIQ Advanced Authentication для защиты VPN-доступа

➔ Сервер RADIUS

Включено ВКЛ

Тип события

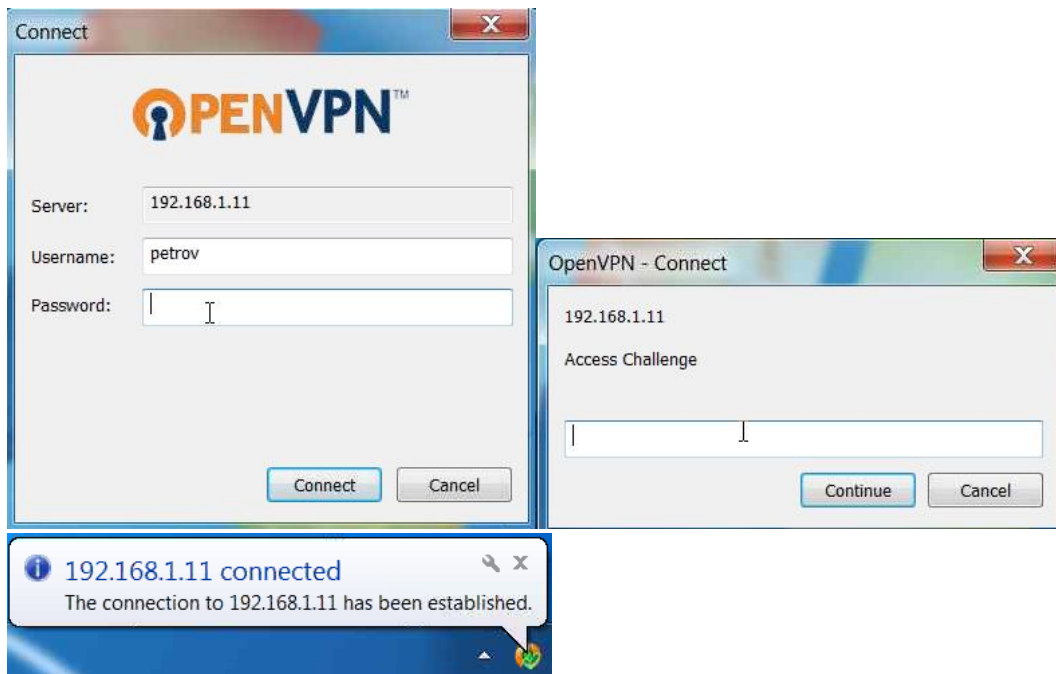
Цепочки

Доступно	Использованные
LDAP Password Only Password Only	LDAP Password & TOTP

Белый список конечных точек

Клиенты

IP-адрес	Имя	Включено	
192.168.1.11	OpenVPN	✓	<input type="checkbox"/> <input type="checkbox"/>



Аналогичным образом решение можно настроить если в организации уже реализована поддержка каких-либо аппаратных токенов (таких, например, как RSA или Vasco). NetIQ Advanced Authentication в данной схеме может выступать в качестве RADIUS-клиента, перенаправляя запросы на проверку подлинности соответствующему RADIUS-серверу, предоставляемому производителем токенов. Такое применение позволяет, с одной стороны, пользоваться преимуществами универсальности решения от Micro Focus, а с другой стороны, защитить инвестиции в существующую инфраструктуру токенов.

Использование многофакторной аутентификации для тонкой настройки доступа к ресурсам

NetIQ Advanced Authentication содержит ряд возможностей для детального разграничения доступа к ресурсам организации. Одним из примеров является компонент Logon Filter, устанавливаемый на контроллер домена Microsoft Active Directory и используемый для поддержки динамических групп. Суть его работы состоит в использовании факта успешной аутентификации через NetIQ Advanced Authentication в качестве обязательного условия предоставления доступа к файлам, папкам, веб-приложениям и прочим ресурсам. После проверки подлинности пользователя Logon Filter добавляет в его токен группу, указывающую на упомянутый факт; затем эту группу можно использовать для настройки правил доступа к ресурсам. В качестве примера приведём ситуацию, когда пользователь должен обязательно аутентифицироваться на своей рабочей станции посредством методов NetIQ Advanced Authentication, чтобы получить возможность

взаимодействовать с сетевой папкой, содержащей конфиденциальную информацию. Если этот пользователь зайдёт под своей учётной записью (и попытается открыть указанную папку) с другого компьютера, то ему будет отказано в доступе.

Ещё одним показателем того, что NetIQ Advanced Authentication может применяться для ограничения доступа к ресурсам, является поддержка им различных стандартов бесконтактных смарт-карт (например, Mifare, EM-Marine, HID). Это будет удобно организациям, использующим такие смарт-карты для доступа в офисные помещения. С помощью NetIQ Advanced Authentication можно настроить те же самые смарт-карты для доступа к рабочим станциям. Поскольку сотрудники в офисе всегда носят корпоративные бейджи с собой (иначе они не смогут выйти из комнаты), можно существенно повысить безопасность, настроив автоматическую блокировку сессии на рабочей станции при снятии смарт-карты со считывателя.

Индивидуализация решения посредством API и SDK

Несмотря на наличие большого количества функциональности «из коробки», NetIQ Advanced Authentication предоставляет разработчикам технический инструментарий для расширения имеющихся возможностей. Во-первых, документация продукта содержит опубликованный REST API, с помощью которого получится, например, индивидуализировать портал настройки аутентификаторов для пользователей. Кроме того, в NetIQ Advanced Authentication имеется мобильный SDK. Его можно использовать для разработки собственного мобильного приложения, в котором будут показываться одноразовые пароли или пуш-уведомления.

Готовые интеграции с IAM-продуктами NetIQ от Micro Focus

Важной особенностью решений NetIQ является полнота портфеля IAM и наличие многочисленных готовых механизмов взаимодействия между его составляющими. Вот некоторые примеры «коробочных» интеграций NetIQ Advanced Authentication:

- Интеграция с решением по контролю привилегированных пользователей NetIQ Privileged Account Manager. Подтверждает личность пользователя прежде предоставления ему привилегированного доступа к серверам или приложениям, даёт дополнительную защиту в случае компрометации учётных данных.

- Интеграция с решением по управлению доступом к веб-ресурсам NetIQ Access Manager. Обеспечивает должный уровень безопасности при единой аутентификации и сквозном доступе к локальным и облачным веб-сервисам.

- Интеграция с решением по сквозной аутентификации NetIQ SecureLogin. Дополнительные методы проверки подлинности NetIQ Advanced Authentication могут быть использованы при получении доступа к традиционным приложениям через «толстый клиент».

- Интеграция с решением по автоматизации самостоятельной смены паролей NetIQ Self-Service Password Reset. Позволяет при запросе на сброс пароля удостовериться в подлинности пользователя за счёт дополнительных факторов аутентификации.

Таким образом, хотя каждый из перечисленных продуктов можно применять по отдельности, их совместное использование несёт очевидные выгоды: простота интеграции (не нужно ничего самостоятельно писать), минимизация «стыковочных» рисков, наличие технической поддержки всего интеграционного решения от одного вендора.

Интеграция с риск-сервисом от Micro Focus

Одним из нововведений в линейке решений NetIQ IAM от Micro Focus является т. н. «риск-сервис». Суть его заключается в следующем. При поступлении запроса из приложения NetIQ (среди прочих поддерживается и NetIQ Advanced Authentication) система на основе сопутствующей контекстной информации вычисляет уровень риска, связанный именно с этим запросом на доступ.

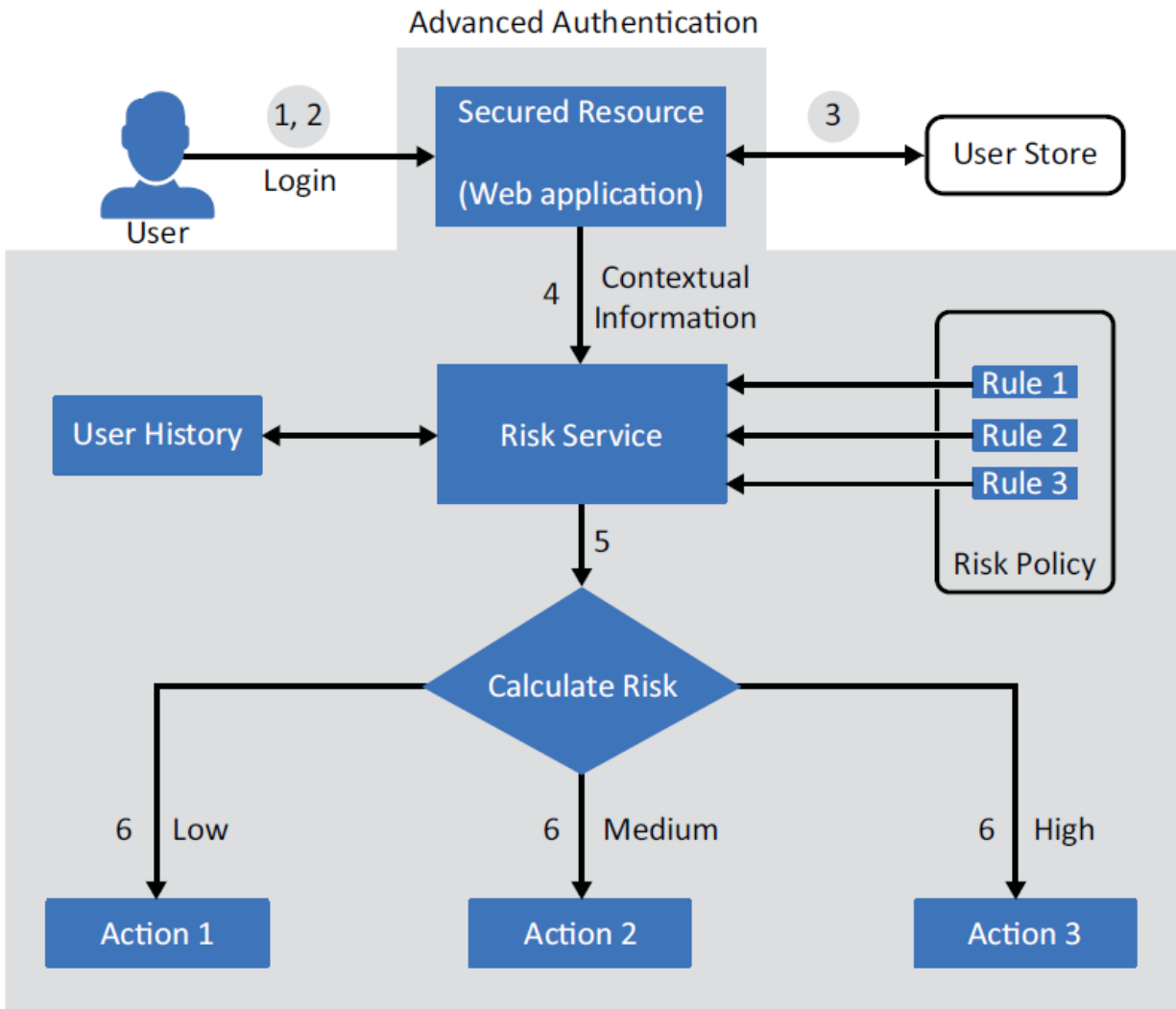
Примеры контекстных параметров для вычисления уровня риска:

- IP-адрес, с которого поступил запрос;
- пользовательские файлы идентификации (cookies);
- содержимое HTTP-заголовка запроса;
- история предыдущих запросов пользователя;
- внешние параметры (доступ через REST API, вызовы во внешние системы и т. п.).

В зависимости от заданных пороговых значений сервис относит риск, связанный с данным запросом, к одной из трёх категорий: низкий, средний или высокий уровень риска. В случае NetIQ Advanced Authentication для каждой такой категории у пользователя запрашивается та или иная цепочка методов аутентификации. Например, для доступа к одной и той же системе можно настроить как простые цепочки (скажем, с отправкой одноразовых паролей на смартфон), так и более строгие (с подтверждением личности

через аппаратный токен или даже биометрические данные). Это позволит соблюсти баланс между удобством доступа для пользователя и обеспечением должного уровня безопасности.

Рисунок 14. Схема работы NetIQ Advanced Authentication с риск-сервисом от Micro Focus



Выводы

Актуальные тенденции в области цифровизации ведут к наращиванию объёмов удалённой работы и к размыванию традиционных корпоративных периметров. Пандемия нового коронавирусного заболевания в 2020 году дополнительно ускорила эти процессы. В таких условиях особенно важно обеспечить надёжную аутентификацию сотрудников, подключающихся к информационным ресурсам компании или ведомства извне.

С помощью NetIQ Advanced Authentication от Micro Focus можно организовать многофакторную аутентификацию в организации, задействовав разнообразные методы и совокупности факторов для различных ситуаций и сценариев применения. Масштабируемая архитектура с отказоустойчивостью позволит развернуть решение и на малой, и на крупной инфраструктуре, а возможности интеграции и индивидуализации (в том числе — через REST API и мобильный SDK) помогут приспособиться к уже внедрённым информационным системам.