ZTNA VS VPN: АНТИПОДЫ ИЛИ ДРУЗЬЯ?

Вячеслав САВЛЮК
генеральный директор компании ИТ-Экспертиза

Артём ТУРЕНОК
руководитель отдела технических решений АО «ДиалогНаука»

Стратегия ZTNA (Zero Trust Network Access) сейчас на слуху. Причём она довольно часто противопоставляется старым добрым технологиям VPN (Virtual Private Network). В качестве аргумента чаще всего приводится такое утверждение: в отличие от VPN, которые предоставляют полный доступ к локальной сети, решения на базе ZTNA предпочитают никому не доверять, разрешая доступ только к тем услугам или ресурсам, которые пользователи явно запросили.

Кроме этого, бытует мнение, что у VPN неэффективная производительность: например, концентраторы VPN могут создавать узкие места, что приводит к снижению производительности, чрезмерной задержке в обменах информацией и тому подобным неприятностям. Порой настройка VPN — дорогая и трудоёмкая процедура, требующая больших усилий со стороны службы безопасности и самих пользователей.

В общем, «*переходите все на ZTNA, и будет вам счастье*». Так ли это? Неужели пришло время списывать со счетов проверенный временем VPN? Давайте порассуждаем на эту тему.

А ЧТО ТАКОЕ ZTNA

В стратегии ZTNA доступ к ресурсам и приложениям предоставляется на основе строгой аутентификации и авторизации. Каждый пользователь и каждое устройство должны пройти проверку и авторизацию перед получением доступа к ресурсам. А сами пользователи и устройства имеют только те привилегии, которые необходимы для выполнения их конкретных задач. Всё это уменьшает вероятность несанкционированного доступа и помогает предотвратить вредоносные действия.

Но, прежде чем говорить о ZTNA дальше, окунёмся в историю. Считается, что идея Zero Trust («нулевого доверия») была придумана в 2010 году аналитиком Forrester. При этом в России парадигма «доверенной среды» появилась лет на 25 раньше. Несмотря на противоположные названия, есть много объединяющих их критериев (разрешено: только определенное ПО, процессы, определены ресурсы, к которым предоставляется доступ).

Есть и отличия: главный тезис концепции «доверенной среды» — если мы сможем быть уверенными в надёжности (лояльности, доверенности) каждого элемента, нам не обязательно изолировать их в замкнутой среде. В силу принципа декомпозиции, каждый элемент защищаемой информационной системы сам по себе может быть защищён, и в этом случае соединение их в единую информационную систему с помощью защищённых каналов позволит создать вокруг информации надёжную оболочку.

«Доверенная среда» предполагает, что должно быть доверие:

- к окружению системы;
- к субъектам отношений;
- к правилам и процедурам;
- к аппаратной и программной платформе;
- к выполняемым операциям;
- к каналам передачи информации.

Достичь требуемого уровня доверия возможно, если обеспечивается:

- локализация информационных ресурсов;
- счётность субъектов и объекты доступа;
- доверенность конфигурации и настройки;
- целостность всех элементов;
- подконтрольность всех действий;
- логирование всех событий.

Иными словами, для реализации концепции «доверенной среды» в информационной системе должен быть создан специальный сегмент, имеющий защиту по всему периметру и не позволяющий постороннему бесконтрольно обращаться с информацией.

Вернёмся к стратегии ZTNA. Она предполагает создание вокруг приложения или группы приложений логической границы доступа на основе идентификации и контекста, то есть учёта группы или роли пользователя, его IP-адреса, местоположения и временных ограничений. Цель ZTNA заключается в обеспечении безопасного доступа к ресурсам и приложениям в сети вне зависимости от расположения устройства или пользователя.

Стратегия ZTNA предполагает:

- каждое устройство, пользователь и приложение должны быть проверены и авторизованы перед получением доступа к ресурсам в сети. Нет доверия к устройству или пользователю на основе их сетевого положения или предыдущих разрешений;
- сеть разделяется на отдельные микросегменты (микропериметры), где доступ к ресурсам и приложениям строго контролируется. Каждое соединение и каждый запрос должны быть аутентифицированы и авторизованы на уровне микросегмента. Это позволяет ограничить доступ к ресурсам только для необходимых пользователей и устройств и минимизировать поверхность атаки;

- для получения доступа к ресурсам требуется не только пароль, но и учет контекста, такого как атрибуты пользователя, идентификация устройства, контекст подключения и другие факторы.

В принципе, обе точки зрения говорят о схожих сущностях. Но традиционно «дьявол кроется в деталях».

С точки зрения «нулевого доверия» прежде всего требуется постоянный мониторинг и управление доступом и привилегиями пользователей, а также мониторинг всего трафика на предмет вредоносных действий. И здесь остается открытым вопрос доверия к конечному оборудованию пользователя.

С точки зрения «доверенной среды» требуется постоянный мониторинг конфигураций, настроек и целостности рабочих мест. То есть прежде всего — формирования доверия к компьютеру конкретного пользователя.

Ну, а процедура идентификации — аутентификации — авторизации в обоих случаях является обязательной.

Обратите внимание на две весьма схожие сущности: в одном случае говорится о сегментировании сети (локализации обрабатываемой информации), в другом — о микросегментах (собственно локализации приложений).

СЛАБОЕ ЗВЕНО

Между тем, во всех описаниях стратегии ZTNA, в отличие от концепции «доверенной среды», не упоминается об одном важном элементе. Посмотрите внимательно: есть удалённый (хотя не обязательно) пользователь, которого проверили со всем пристрастием. Компьютер его тоже опознали: идентифицировали и проверили все его параметры. А ещё есть микросегмент сети, в котором находится нужное пользователю приложение.

Получаются две доверенные сущности. И тут встает вопрос: а как эти сущности взаимодействуют? По всей вероятности, здесь требуется какой-то защищенный (доверенный) канал, тем более что общение сущностей идет через заранее агрессивную среду.

На сегодня наиболее эффективным для этих целей признается шифрование. Но ведь не все приложения имеют криптографическую функцию. И тогда канал связи без криптографии оказывается самым слабым звеном защиты.

Чтобы устранить эту брешь, строго следуя стратегии ZTNA, потребуется на границе каждого микросегмента ставить некое устройство, позволяющее обеспечить шифрованный обмен информацией между пользователем и выбранным приложением.

А если пользователь использует несколько приложений или несколько пользователей из разных мест хотят задействовать одно и то же приложение, что делать? Представляете, насколько это усложнит систему?!

Однако выход из этой ситуации есть. Надо построить «толстый» канал, защищенный криптографией, между пользователем и периметром сети, а уже дальше применять стратегию ZTNA. Ну а чем это отличается от классического VPN? Вот и получается, что одно без другого не даст желаемого результата.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ

Для того чтобы обеспечить контекстную аутентификацию, вначале надо провести инвентаризацию удалённого компьютера, создать некий его профиль и в дальнейшем с регулярной периодичностью отслеживать его состояние, настройки, конфигурацию, целостность.

То есть необходимо в режиме реального времени проводить мониторинг:

- ГДЕ находится компьютер;
- КАК подключается компьютер;
- ЧТО установлено на компьютере;
- ЧТО запущено на компьютере;
- ЧТО делает пользователь.

При этом средство мониторинга должно как минимум уметь контролировать:

- геолокацию компьютера и структуру информационной сети;
- состав программного и аппаратного обеспечения;
- параметры настройки операционной системы, версионность, обновления;
- наличие установленных средств защиты информации, их параметры и включенные компоненты защиты;
- установку, настройку, актуальность программного обеспечения;
- тип и состав подключенных USB устройств;
- запущенные в операционной системе процессы;
- процедуры logon/logoff пользователей.

Сведения обо всех этих параметрах как раз и будут составлять профиль рабочего места. Но пассивное наблюдение вряд ли даст положительный эффект. Необходимо не только контролировать, но и иметь возможность управлять рабочим местом: уведомлять администратора безопасности об отклонениях, блокировать доступ в критических ситуациях или переводить компьютер в карантин.

Однако и этого мало. Нужно правильно построить хранилище, в котором и должен храниться тот самый профиль рабочего места, с которым будет проводиться сравнение. Это и будет корень доверия. Естественно, что такое хранилище должно быть надёжно защищено и исключать всякую возможность изменения профилей.

РЕЗЮМЕ

Применяя новые технологии в защите информации, не надо забывать и о уже проверенных и хорошо себя зарекомендовавших технологиях. Стратегия ZTNA не заменяет VPN, а наоборот предполагает симбиоз этих технологий.

И совокупность технологий, обеспечивающих реализацию стратегии ZTNA, по меньшей мере, но не ограничиваясь, должна позволять выполнять:

- строгую (например, двухфакторную) аутентификацию;
- мониторинг состояния и параметров компьютера пользователя;
- мониторинг состояния и параметров СрЗИ, установленных на компьютере пользователя;
- строгое разграничение полномочий пользователя (например, по мандатному принципу);
- создание защищённых каналов связи (например, применение VPN);
- возможность блокировки подключения компьютера пользователя к сети в случае нарушения установленной политики его использования.