Безопасность Windows 7. DirectAccess

> Тарас Злонов, CIO-World, 12 марта 2009 года

В рамках цикла статей, посвящённых новым решениям в Windows 7, связанным с информационной безопасностью, мы уже не раз упоминали серверную операционную систему Windows Server 2008 R2.

Действительно, эта пара операционных систем, основанная во многом на одном и том же ядре, будет представлять собой идеальное сочетание, каковым сейчас является Windows Vista SP1 и Windows Server 2008. Дело в том, что некоторые новые технологии Microsoft доступны исключительно при “правильном сочетании” клиентской и соответствующей серверной операционных системах.

Одним из примеров такого “синергетического эффекта” является новая технология от Microsoft - DirectAccess, которая становится доступной при одновременном использовании в компании рабочих станций под управлением Windows 7 и серверов с ОС Windows Server 2008 R2.

Основное предназначение DirectAccess такое же, как у виртуальных частных сетей (VPN - Virtual Private Network), а именно - предоставление защищённого соединения с корпоративной сетью для удалённых пользователей, работающих через публичные сети (чаще всего - Интернет).

Основное отличие DirectAccess от VPN состоит в том, что безопасное соединение устанавливается в фоновом режиме без участия пользователя. Такой подход позволяет сделать максимально простой и удобной работу удалённых мобильных пользователей без снижения обеспечиваемого уровня безопасности. Устанавливаемое автоматически защищённое соединение не требует повторного ручного подключения, даже если связь с сетью Интернет прерывается, а групповые политики теперь могут применяться ещё до входа пользователя в ОС. То же самое касается и процедур установки обновлений программного обеспечения.

С помощью DirectAccess устанавливается защищённое двунаправленное соединение с использованием протоколов IPv6 (Интернет протокол версии 6 - Internet Protocol version 6) и IPsec (безопасный интернет-протокол - Internet Protocol Security). Последний позволяет использовать для шифрования передаваемого трафика алгоритмы Triple Data Encryption Standard (3DES) или Advanced Ensryption Standard (AES).

Принципиальная схема подключения изображена на рисунке.

> **Добавлено 04.08.2020**
> За давностью лет рисунок, к сожалению, утрачен

Компьютер пользователя соединяется с сервером DirectAccess, который выступает в роли своеобразного шлюза для доступа к остальным корпоративным ресурсам. При этом клиент DirectAccess, являющийся частью Windows 7, устанавливает два соединения с использованием IPSec ESP (Протокол безопасного закрытия содержания - Encapsulating Security Payload):

- IPSec ESP тоннель с использованием сертификата компьютера для обеспечения соединения с корпоративным DNS сервером и контроллером домена, который позволяет применять к компьютеру групповые политики до входа пользователя в ОС;
- IPSec ESP тоннель с одновременным использованием сертификата компьютера и учётных данных пользователя для предоставления доступа к внутренним корпоративным ресурсам и приложениям.

При большом количестве внешних пользователей для серверов DirectAccess может применятся технологии кластеризации и балансировки нагрузки.

Важным преимуществом DirectAccess является возможность разделения “корпоративного” трафика и трафика, предназначенного для внешних Интернет серверов. Благодарая этому DirectAccess, в отличие от VPN, автоматически снижает нагрузку на корпоративные сервера, за счёт перенаправления интернет-трафика в обход установленных защищённых соединений.

DirectAccess производит аутентификацию компьютера ещё до входа пользователя в операционную систему, предоставляя доступ к DNS серверам и контроллерам домена. При последующей аутентификации пользователя ему предоставляются права доступа к другим внутренним ресурсам компании. При этом, помимо стандартной аутентификации пользователя по имени и паролю, для обеспечения более высокого уровня безопасности может использоваться двухфакторная аутентифкация с применением смарт-карт, что существенно снижает вероятность компрометации учётных данных пользователя. При использовании DirectAccess смарт-карты могут применяться для аутентификации пользователя вне зависимости от используемого им компьютера, аутентификации компьютера вне зависимости от работающего за ним пользователя и дополнительной аутентификации при доступе к конкретным внутренним ресурсам.

Для использования DirectAccess желательна поддержка современного протокола IPv6, но, также допустима работа с использованием IPV4 или teredo IPv6, которые позволяют инкапсулировать трафик IPv6 в широко распространённый сегодня IPv4.

При необходимости проверки состояния подключаемых к корпоративной сети компьютеров для снижения вероятности воздействия вредоносных программ на защищённость информационных ресурсов компании DirectAccess позволяет использовать технологии NAP (Network Access PROTECTION - безопасность сетевого доступа) и NAC (Network Access Control - контроль сетевого доступа).

Так, например, для предоставления возможности подключения к корпоративной сети можно потребовать наличия на компьютере пользователя актуальных обновлений операционной системы, актуальных антивирусных баз и соответствия другим политикам безопасности. Компьютер пользователя, заражённый вирусом, не сможет получить доступа к корпоративным ресурсам, что ограничит распространение вирусной эпидемии. Использование NAP и NAC совместно с DirectAccess не является обязательным условием, но крайне рекомендуется корпорацией Microsoft для максимального уровня обеспечения информационной безопасности.

Таким образом, для полноценного использования DirectAccess необходима соответствующая инфраструктура, в составе которой потребуются:

- Сервер DirectAccess на базе ОС Windows Server 2008 R2;
- Клиент DirectAccess на рабочей станции и Windows 7;
- Два сетевых интерфейса на сервере для соединения с внешней (Интернет) и внутренней (Интранет) сетями;
- Инфраструктура открытых ключей (PKI - Public Key Infrastructure);
- Домен на базе Active Directory;
- Поддержка протокола IPv6;
- NAC и/или NAP решения.

Такие технологии, как DirectAccess, напрямую направлены на дальнейшее развитие “облачных” вычислений, ставших столь популярными в последнее время. Суть облачных вычислений состоит в том, чтобы предоставлять пользователю сервисы вне зависимости от его местонахождения. С учётом того, что скорости и пропускные способности каналов связи для мобильных устройств существенно выросли за последнее время и продолжают возрастать, всё больше и больше пользователей не будут замечать разницы при работе внутри стен офиса или далеко за его пределами.

С помощью DirectAccess администраторы получают возможность удалённо управлять компьютерами организации вне зависимости от того, где в данный момент физически находится рабочая станция пользователя - в офисе, на другом краю света или существует в виде файла виртуальной машины в дата-центре. Сочетание современных технологий позволит получить основные преимущества масштабируемости, мобильности и мощности вычислений.

DirectAccess - очень интересное решение. Вполне возможно, что со временем оно полностью вытеснит VPN. Действительно, возможность без дополнительной головной боли получать доступ к корпоративным файловым серверам, внутренним веб-сайтам и приложениям существенно облегчит жизнь как самим пользователям, так и администраторам - за счёт уменьшения времени, которое сейчас затрачивается на разъяснения и помощь при подключении к VPN-серверам.