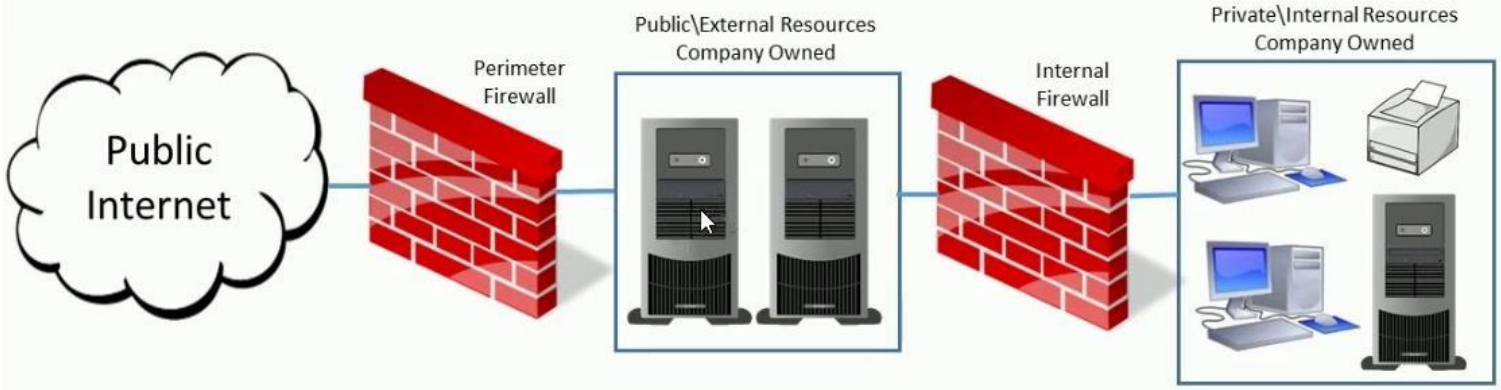
# DMZ (Demilitarized Zone)




**DMZ** (*Demilitarized Zone* — демилитаризованная зона, ДМЗ) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.

Цель ДМЗ — добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

# Архитектура и реализация

Разделение сегментов сети и фильтрация трафика между ними, как правило, реализуются специализированными устройствами — межсетевыми экранами. Основными задачами такого устройства являются:

- контроль доступа из внешней сети в ДМЗ;
- контроль доступа из внутренней сети в ДМЗ;
- разрешение (или контроль) доступа из внутренней сети во внешнюю;
- запрет доступа из внешней сети во внутреннюю.

В некоторых случаях для организации ДМЗ достаточно средств маршрутизатора или даже прокси-сервера.

Серверы в ДМЗ при необходимости могут иметь ограниченную возможность соединиться с отдельными узлами во внутренней сети. Связь в ДМЗ между серверами и с внешней сетью также ограничивается, чтобы сделать ДМЗ более безопасной для размещения определённых сервисов, чем Интернет. На серверах в ДМЗ должны выполняться лишь необходимые программы, ненужные отключаются или вообще удаляются.

Существует множество различных вариантов архитектуры сети с DMZ. Два основных — с одним межсетевым экраном и с двумя межсетевыми экранами. На базе этих методов можно создавать как упрощенные, так и очень сложные конфигурации, соответствующие возможностям используемого оборудования и требованиям к безопасности в конкретной сети.

# Конфигурация с одним межсетевым экраном

- Для создания сети с ДМЗ может быть использован один межсетевой экран, имеющий минимум три сетевых интерфейса: один — для соединения с провайдером (WAN), второй — с внутренней сетью (LAN), третий — с ДМЗ. Подобная схема проста в реализации, однако предъявляет повышенные требования к оборудованию и администрированию: межсетевой экран должен обрабатывать весь трафик, идущий как в ДМЗ, так и во внутреннюю сеть. При этом он становится единой точкой отказа, а в случае его взлома (или ошибки в настройках) внутренняя сеть окажется уязвимой напрямую из внешней.

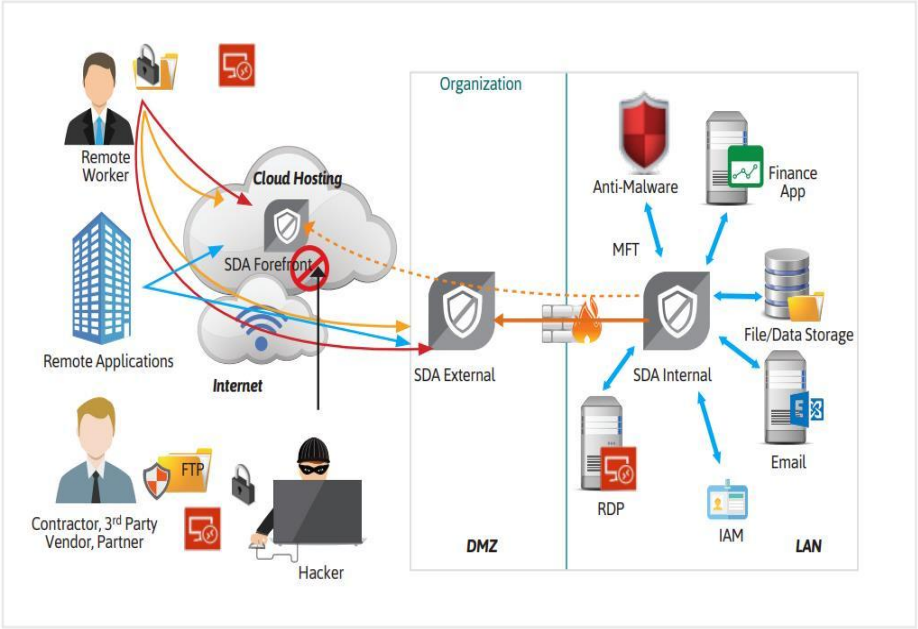
# Конфигурация с двумя межсетевыми экранами

- Более безопасным является подход, когда для создания ДМЗ используются два межсетевых экрана: один из них контролирует соединения из внешней сети в ДМЗ, второй — из ДМЗ во внутреннюю сеть. В таком случае для успешной атаки на внутренние ресурсы должны быть скомпрометированы два устройства. Кроме того, на внешнем экране можно настроить более медленные правила фильтрации на уровне приложений, обеспечив усиленную защиту локальной сети без негативного влияния на производительность внутреннего сегмента.
- Ещё более высокий уровень защиты можно обеспечить, используя два межсетевых экрана двух разных производителей и (желательно) различной архитектуры — это уменьшает вероятность того, что оба устройства будут иметь одинаковую уязвимость Например, случайная ошибка в настройках с меньшей вероятностью появится в конфигурации интерфейсов двух разных производителей; дыра в безопасности, найденная в системе одного производителя, с меньшей вероятностью окажется в системе другого. Недостатком этой архитектуры является более высокая стоимость.

# ДМЗ-хост

Некоторые маршрутизаторы SOHO-класса имеют функцию предоставления доступа из внешней сети к внутренним серверам (режим *DMZ host* или *exposed host*). В таком режиме они представляют собой хост, у которого открыты (не защищены) все порты, кроме тех,
которые транслируются иным способом. Это не вполне соответствует определению истинной ДМЗ, так как сервер с открытыми портами не отделяется от внутренней сети. То есть ДМЗ-хост может свободно подключиться к ресурсам во внутренней сети, в то время как соединения с внутренней сетью из настоящей ДМЗ блокируются разделяющим их межсетевым экраном, если нет специального разрешающего правила. ДМЗ-хост не предоставляет в плане безопасности ни одного из преимуществ, которые даёт использование подсетей, и часто используется как простой метод трансляции всех портов на другой межсетевой экран или устройство.

# Технология Reverse Access




Подход от компании Safe-T — технология Reverse Access — сделает DMZ еще более безопасной. Эта технология, основанная на использовании двух серверов, устраняет необходимость открытия любых портов в межсетевом экране, в то же самое время обеспечивая безопасный доступ к приложениям между сетями (через файрвол). Решение включает в себя:

- Внешний сервер — устанавливается в DMZ / внешнем / незащищенном сегменте сети.
- Внутренний сервер — устанавливается во внутреннем / защищенном сегменте сети.

# Технология Reverse Access

Роль внешнего сервера, расположенного в DMZ организации (на месте или в облаке), заключается в поддержании клиентской стороны пользовательского интерфейса (фронтенда, front-end) к различным сервисам и приложениям, находящимися во Всемирной сети. Он функционирует без необходимости открытия каких-либо портов во внутреннем брандмауэре и гарантирует, что во внутреннюю локальную сеть могут попасть только легитимные данные сеанса. Внешний сервер выполняет разгрузку TCP, позволяя поддерживать работу с любым приложением на основе TCP без необходимости расшифровывать данные трафика криптографического протокола SSL (Secure Sockets Layer, уровень защищенных сокетов).

Роль внутреннего сервера заключается в том, чтобы провести данные сеанса во внутреннюю сеть с внешнего узла SDA (Software-Defined Access, программно-определяемый доступ), и, если только сеанс является легитимным, выполнить функциональность прокси-сервера уровня 7 (разгрузка SSL, переписывание URL-адресов, DPI (Deep Packet Inspection, подробный анализ пакетов) и т. д.) и пропустить его на адресованный сервер приложений.

Технология Reverse Access позволяет аутентифицировать разрешение на доступ пользователям еще до того, как они смогут получить доступ к вашим критически-важным приложениям. Злоумышленник, получивший доступ к вашим приложениям через незаконный сеанс, может исследовать вашу сеть, пытаться проводить атаки инъекции кода или даже передвигаться по вашей сети. Но лишенный возможности позиционировать свою сессию как легитимную, атакующий вас злоумышленник лишается большей части своего инструментария, становясь значительно более ограниченным в средствах.

# Безопасность DMZ

Владельцам в ДМЗ разрешено иметь ограниченное подключение к определенным узлам внутренней сети, поскольку содержимое ДМЗ не так безопасно, как содержимое внутренней сети. Аналогичным образом, связь между узлами DMZ и внешней сетью также ограничена, чтобы сделать DMZ более безопасной, чем Интернет, и пригодной для размещения этих служб специального назначения. Это позволяет узлам DMZ взаимодействовать как с внутренней, так и с внешней сетью, в то время как промежуточный брандмауэр контролирует трафик между серверами DMZ и клиентами внутренней сети, а другой брандмауэр будет выполнять некоторую степень контроля для защиты DMZ от внешней сети.

# Безопасность DMZ

Конфигурация DMZ обеспечивает дополнительную защиту от внешних атак, но обычно не влияет на внутренние атаки, такие как прослушивание связи через анализатор пакетов или подделка, например, подделка электронной почты. Также иногда целесообразно настроить отдельную Классифицированную милитаризованную зону (CMZ) - милитаризованную зону с высоким уровнем мониторинга, состоящую в основном из веб-серверов (и аналогичных серверов, взаимодействующих с внешним миром, т. е. Интернетом), которые не находятся в DMZ, но содержат важную информацию о доступе к серверам в ЛВС (таким как серверы баз данных). В такой архитектуре DMZ обычно имеет брандмауэр приложения и FTP, в то время как CMZ содержит веб-серверы. (Серверы баз данных могут находиться в CMZ, в локальной сети или в отдельной VLAN вообще).Любая услуга, предоставляемая пользователям во внешней сети, может быть размещена в DMZ. Наиболее распространенными из них являются следующие:

- веб-серверы
- Почтовые серверы
- FTP-серверы
- VoIP-серверы