**DMZ**

**DMZ (Demilitarized Zone, 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.

Разделение сегментов и контроль 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.