Топология сети при использовании межсетевых экранов

- DMZ-сеть
- Принципы построения окружения межсетевого экрана
- Архитектура с несколькими уровнями межсетевых экранов
  - Конфигурация с одной DMZ-сетью
  - Service Leg конфигурация
  - Конфигурация с двумя DMZ-сетям
  - Конечные точки VPN
  - Расположение серверов в DMZ-сетях

Топология сети при использовании межсетевых экранов

- Межсетевые экраны используются для разграничения сетей, имеющих **разные требования к безопасности**.
- Межсетевые экраны следует использовать каждый раз, когда внутренние сети и системы взаимодействуют с внешними сетями и системами и когда требования безопасности различаются в нескольких внутренних сетях.
- Рассмотрим, где должны быть расположены межсетевые экраны и как должны быть расположены другие сети и системы относительно межсетевых экранов.
- Так как первоначальной функцией межсетевого экрана является предотвращение нежелательного входящего трафика в сеть (и в некоторых случаях исходящего), межсетевые экраны должны быть расположены в точках входа на логических границах сети.
- Обычно это означает, что межсетевой экран является узлом, в котором **сетевой трафик разделяется на несколько путей, либо собирается вместе в единственный путь**.

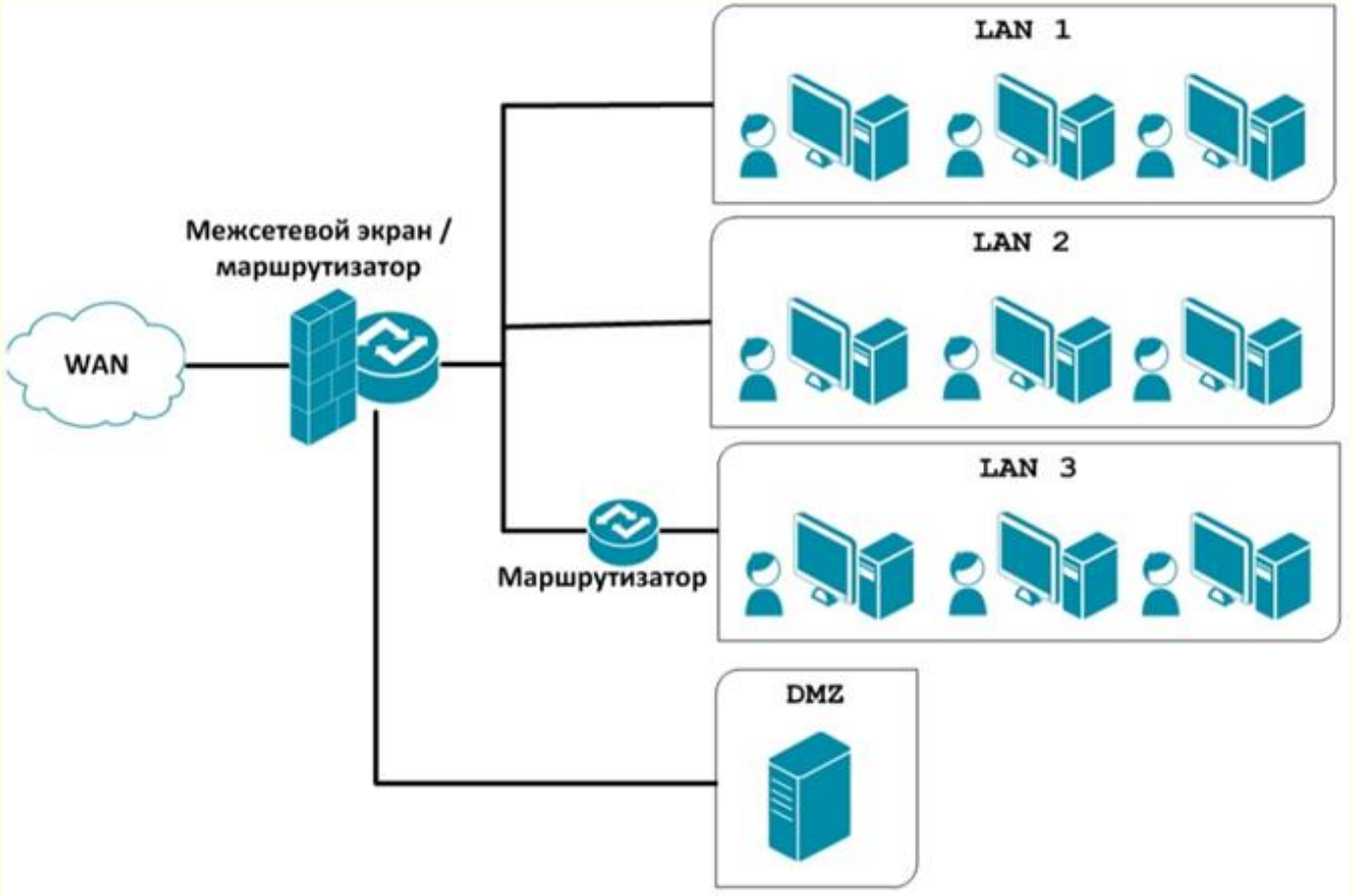
Топология сети при использовании межсетевых экранов

- При маршрутизации межсетевой экран обычно расположен непосредственно перед маршрутизатором и иногда совмещается с маршрутизатором.
- Гораздо реже межсетевой экран располагается после разделения трафика на несколько маршрутов, потому что в этом случае межсетевой экран должен будет следить за каждым из этих маршрутов.
- Часто аппаратные устройства межсетевого экранирования имеют также и возможности маршрутизации, и в сетях, построенных с использованием коммутаторов, межсетевой экран часто является частью самого коммутатора, что обеспечивает возможность защищать все коммутируемые сегменты.

Топология сети при использовании межсетевых экранов

- Межсетевой экран получает трафик, проверяет его в соответствии со своей политикой и выполняет соответствующее действие (например, пропускает трафик, блокирует его, выполняет некоторое преобразование).
- Мы уже рассмотрели различные типы технологий межсетевого экранирования.
- Межсетевые экраны, расположенные на границы сетевого периметра, часто являются аппаратными устройствами с несколькими сетевыми интерфейсами; межсетевые экраны для хостов и персональные межсетевые экраны встроены в ПО, которое установлено на одном компьютере, и защищают только данный компьютер; устройства персонального межсетевого экрана предназначены для защиты единственного компьютера или сети небольшого офиса.
- Будем рассматривать только межсетевые экраны, расположенные **на границе сетевого периметра**, потому что для остальных типов не важна топология сети.

DMZ-сеть


LAN 1
LAN 2
LAN 3
Межсетевой экран / маршрутизатор
WAN
Маршрутизатор
DMZ

DMZ-сеть

- Многие аппаратные устройства межсетевого экранирования имеют функциональность, называемую **DMZ** – это сокращение от демилитаризованной зоны, которую устанавливают между воюющими странами.
- Хотя и не существует одного определения для DMZ, обычно **они являются интерфейсами в межсетевом экране, для которых возможно задавать правила маршрутизации**, и аналогичны интерфейсам, расположенным на защищаемой стороне межсетевого экрана.
- Основное различие состоит в том, что трафик, проходящий между DMZ и другими интерфейсами на защищаемой стороне межсетевого экрана, проходит через межсетевой экран, и к нему может **применяться своя политика**.

DMZ-сеть

- DMZ часто используется в том случае, если существуют хосты, которым необходимо, чтобы весь трафик обрабатывался политиками межсетевого экрана (например, для того чтобы хосты в DMZ были бы специально усилены), но трафик от хостов к другим системам в сети также должен проходить через межсетевой экран.
- **В DMZ располагают публично доступные сервера**, такие как веб-сервер или почтовый сервер.
- Трафик из интернета проходит через межсетевой экран и маршрутизируется к системам, расположенным с защищаемой стороны межсетевого экрана, или к системам в DMZ.
- Трафик между системами, расположенными на защищенной стороне, и системами, расположенными в DMZ, проходит через межсетевой экран, и к ним могут применяться политики межсетевого экрана.

Принципы построения окружения межсетевого экрана

1. **Простота (Keep It Simple).** Важно принимать наиболее простые решения – более безопасным является то, чем легче управлять. Трудно понимаемые функциональности часто приводят к ошибкам в конфигурации.
2. **Использовать устройства по назначению.** Например, маршрутизаторы предназначены для выполнения маршрутизации; возможности фильтрования пакетов не являются их исходной целью, и это всегда надо учитывать при разработки окружения межсетевого экрана. Зависимость исключительно от возможности маршрутизатора обеспечивать функциональность межсетевого экрана опасна: он может быть легко переконфигурирован. Другим примером являются сетевые коммутаторы (switch): когда они используются для обеспечения функциональности межсетевого экрана *вне* окружения межсетевого экрана, они чувствительны к атакам, которые могут нарушить функционирование коммутатора. Во многих случаях гибридные межсетевые экраны и аппаратные устройства межсетевых экранов являются лучшим выбором, потому что они оптимизированы в первую очередь для функционирования в качестве межсетевых экранов.

Принципы построения окружения межсетевого экрана

3. **Создавать оборону вглубь.** Оборона вглубь означает создание нескольких уровней защиты в противоположность наличию единственного уровня. Не следует всю защиту обеспечивать исключительно межсетевым экраном. Где может использоваться несколько межсетевых экранов, они должны использоваться. Где маршрутизаторы могут быть сконфигурированы для предоставления некоторого управления доступом или фильтрации, это следует сделать. Если ОС сервера может предоставить некоторые возможности межсетевого экрана, это следует применить.
4. **Уделять внимание внутренним угрозам.** Если уделять внимание только внешним угрозам, то это приводит в тому, что сеть становится открытой для атак изнутри. Хотя это и маловероятно, но следует рассматривать возможность, что нарушитель может как-то обойти межсетевой экран и получить свободу действий для атак внутренних или внешних систем. Следовательно, важные системы, такие, как внутренние веб- или e-mail-серверы или финансовые системы, должны быть размещены позади внутренних межсетевых экранов или DMZ-зон.

Архитектура с несколькими типами межсетевых экранов

Не существует никаких ограничений на то, где можно размещать в сети межсетевой экран.

Межсетевые экраны могут располагаться на входах в границе логической сети, определяя понятия **«внутри»** и **«вне»** относительно межсетевого экрана, но администратор может захотеть иметь дополнительные границы внутри сети и развернуть дополнительные межсетевые экраны для обозначения этих границ.

Использование нескольких уровней межсетевых экранов является типичным способом создания **«эшелонированной обороны»**.

Типичная ситуация, когда требуется несколько уровней межсетевых экранов, расположенных в сети, это наличие внутренних пользователей с различными уровнями доверия.

Архитектура с несколькими типами межсетевых экранов

Например, необходимо защитить базу данных с учетными записями пользователей от сотрудников, которые не должны иметь к ней доступ.

Это можно сделать, размещая **один межсетевой экран на входе в сеть** (предотвращая неограниченный доступ в сеть из интернета) и **другой на входе во внутреннюю сеть**, тем самым определяя границу отдела кадров.

Внутренний межсетевой экран будет блокировать доступ к серверу базы данных любого извне сети отдела кадров, но разрешать ограниченный доступ к другим ресурсам в сети отдела кадров.

Другим типичным примером использования межсетевых экранов внутри сети наряду с межсетевым экранов на входе в сеть является **наличие недоверяемых пользователей**, например, случайных посетителей, которым необходим доступ в интернет.

Часто для посетителей создается возможность беспроводного доступа в сеть.

Межсетевой экран между точками доступа и оставшейся внутренней сетью может предотвратить доступ посетителей в локальную сеть с привилегиями сотрудников.

Архитектура с несколькими типами межсетевых экранов

Расположение межсетевого экрана внутри при наличии межсетевого экрана на входе должно быть тщательно спланировано, чтобы предотвратить случайные ошибки, влияющие на безопасность.

При разработки политики для внутреннего межсетевого экрана могут быть сделаны неправильные предположения, что необходима достаточно слабая политика – например, если администратор внутреннего межсетевого экрана будет считать, что внешний межсетевой экран уже предотвращает основные типы нежелательного трафика, а администратор внешнего межсетевого экрана впоследствии изменит существующую политику, то для хостов за внутренним межсетевым экраном могут возникнуть дополнительные угрозы.

Более хороший подход состоит в дублировании политики внешнего межсетевого экрана.

Это может быть достаточно трудно, если эти межсетевые экраны не имеют возможности автоматически координировать свои политики, что бывает достаточно часто, если межсетевые экраны разработаны разными производителями.

Архитектура с несколькими типами межсетевых экранов

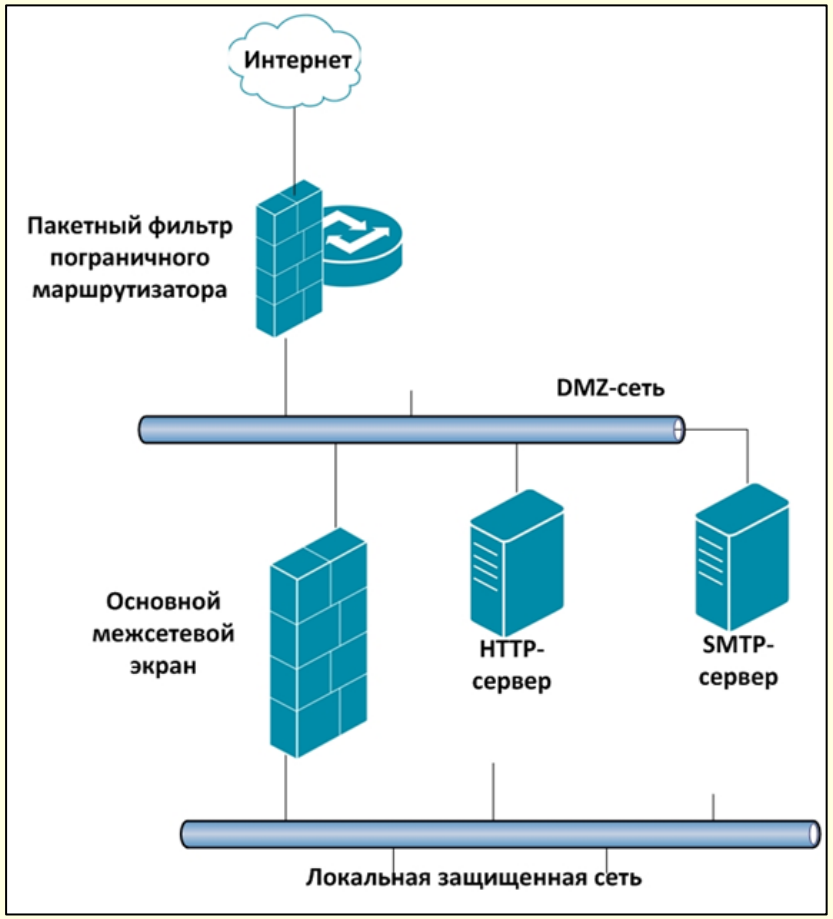
Другой проблемой, связанной с использованием нескольких уровней межсетевых экранов, расположенных в сети, является возрастание сложности трассировки при возникновении каких-либо проблем.

Если между пользователем и сервером находится один межсетевой экран, и пользователь не может соединиться с сервером, то достаточно проверить логи межсетевого экрана.

Но при наличии нескольких межсетевых экранов необходимо определить последовательность их прохождения и проверить все логи.

Наличие нескольких уровней шлюзов прикладного уровня особенно трудно, потому что каждый шлюз может изменить сообщение.

Конфигурация с одной DMZ-сетью



Конфигурация с одной DMZ-сетью

DMZ-сети предназначены для расположения систем и ресурсов, которые не должны быть размещены во внутренних защищенных сетях, но к которым необходим доступ либо только извне, либо только изнутри, либо и извне, и изнутри.

Причина в том, что никогда нельзя гарантировать, что эти системы и ресурсы не могут быть взломаны.

Но взлом этих систем не должен **автоматически означать доступ** ко всем внутренним системам.

DMZ-сети обычно строятся с использованием сетевых коммутаторов и располагаются между двумя межсетевыми экранами или между межсетевым экраном и пограничным маршрутизатором.

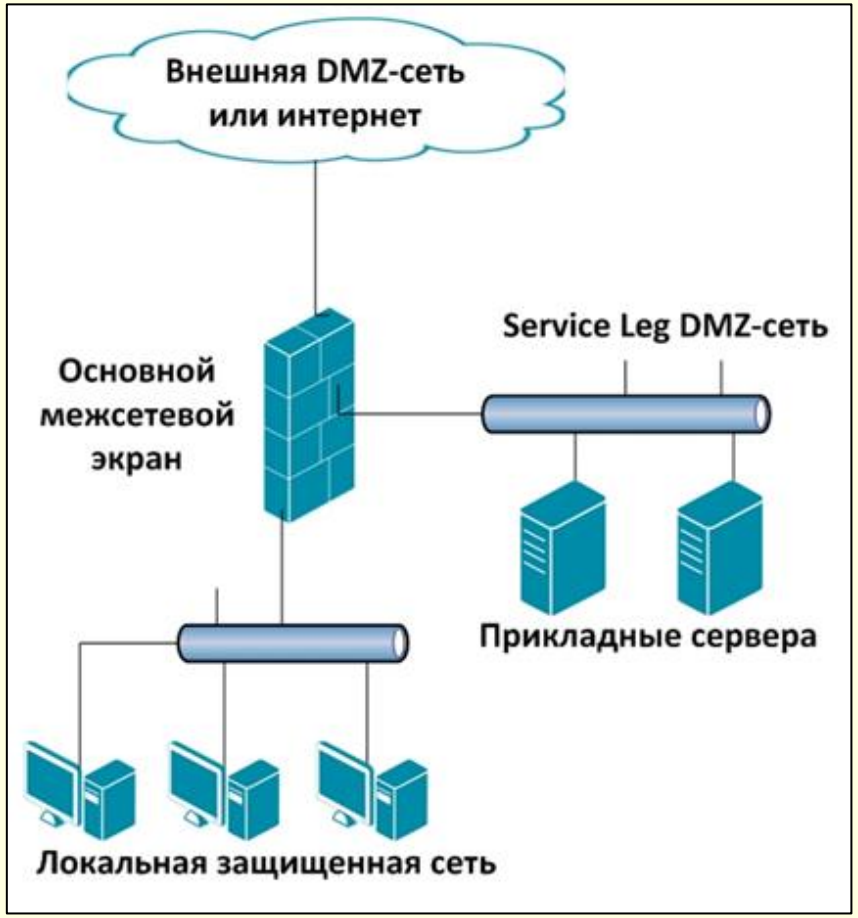
Конфигурация с одной DMZ-сетью

Хорошей практикой является размещение серверов удаленного доступа и конечных точек VPN в DMZ-сетях.

Размещение этих систем в DMZ-сетях уменьшает вероятность того, что удаленные атакующие будут иметь возможность использовать эти серверы в качестве точки входа в локальные сети.

Кроме того, размещение этих серверов в DMZ-сетях позволяет межсетевым экранам служить дополнительными средствами для контроля прав доступа пользователей, которые получают доступ с использованием этих систем к локальной сети.

Service Leg конфигурация



Service Leg конфигурация

Одной из конфигураций DMZ-сети является так называемая **«service leg»** конфигурация межсетевого экрана.

В этой конфигурации межсетевой экран имеет **как минимум три сетевых интерфейса**.

Один сетевой интерфейс соединяется с интернетом, другой соединяется с внутренней сетью, третий сетевой интерфейс формирует DMZ-сеть.

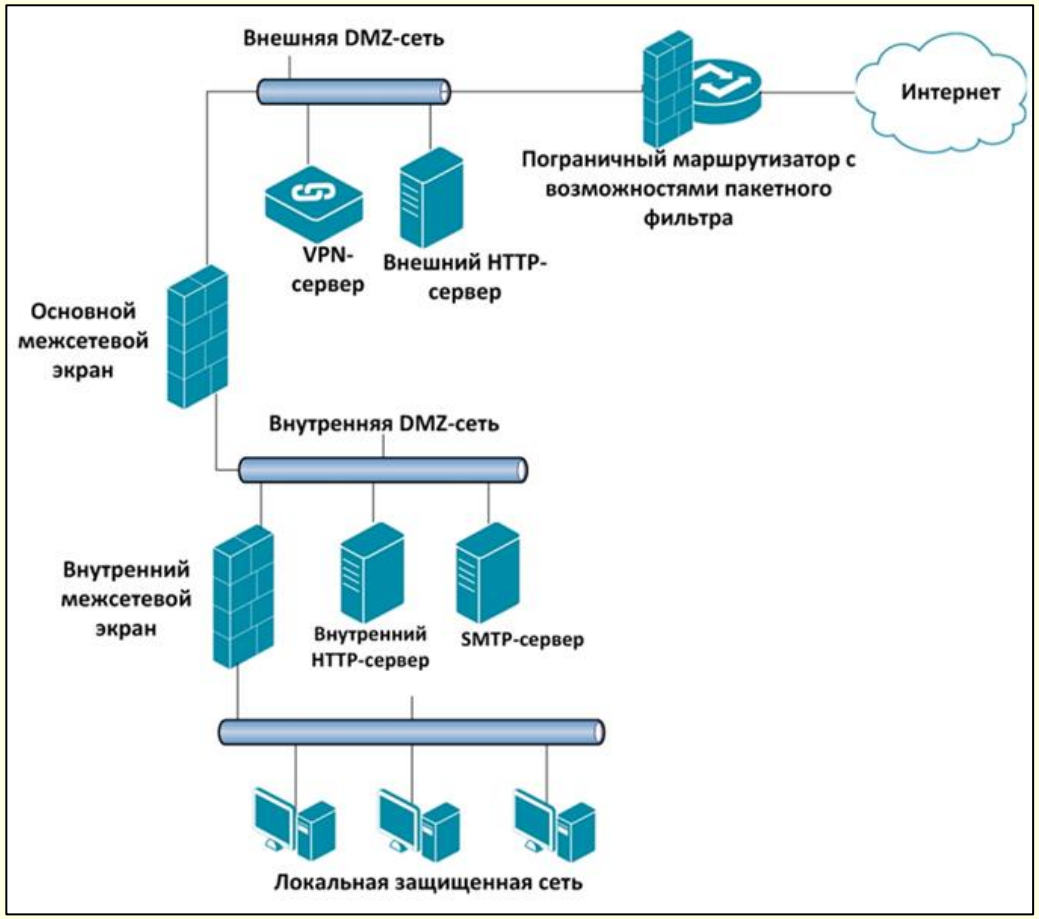
Такая конфигурация может привести к возрастанию риска для межсетевого экрана при DoS-атаке, которая будет нацелена на сервисы, расположенные в DMZ-сети.

В стандартной конфигурации DMZ-сети DoS-атака, направленная на расположенные в DMZ-сети ресурс, такой как веб-сервер, будет воздействовать только на этот целевой ресурс.

В service leg конфигурации DMZ-сети межсетевой экран берет на себя основной удар от DoS-атаки, потому что он должен проверять весь сетевой трафик перед тем, как трафик достигнет расположенного в DMZ ресурса.

В результате это может повлиять на весь трафик организации, если на ее веб-сервер выполнена DoS-атака.

Конфигурация с двумя DMZ-сетями



Конфигурация с двумя DMZ-сетями

При наличии большого числа серверов с разными требованиями доступа можно развернуть межсетевой экран с возможностями пограничного маршрутизатора и два внутренних межсетевых экрана и разместить все внешне доступные серверы во ***внешней*** **DMZ** между маршрутизатором и первым межсетевым экраном.

Пограничный маршрутизатор будет фильтровать пакеты и обеспечивать защиту серверов, первый межсетевой экран будет обеспечивать управление доступом и защиту серверов внутренней DMZ в случае, если внешние сервера атакованы.

Внутренне доступные серверы размещаются во ***внутренней*** **DMZ**, расположенной между основным и внутренним межсетевыми экранами; межсетевые экраны будут обеспечивать защиту и управление доступом для внутренних серверов, защищенных как от внешних, так и от внутренних атак.

Конфигурация с двумя DMZ-сетями

- **Внешняя DMZ-сеть** соединена с интернетом с использованием пакетного фильтра, который одновременно является пограничным маршрутизатором.
- Ранее обсуждалось, почему использование пакетного фильтра является более предпочтительным.
- **Основной межсетевой экран** является VPN-шлюзом для удаленных пользователей; такие пользователи должны иметь ПО VPN-клиента для соединения с межсетевым экраном.
- Входящий SMTP-трафик должен пропускаться основным межсетевым экраном.

Конфигурация с двумя DMZ-сетями

Основной и внутренний межсетевые экраны должны поддерживать технологию анализа состояний и могут также включать возможности прикладного прокси.

Основной межсетевой экран должен выполнять следующие действия:

- **разрешать внешним пользователям**, которые были аутентифицированы VPN-сервером, доступ в локальную сеть и DMZ-сеть;
- если основной межсетевой экран имеет SMTP-прокси, **выполнять фильтрацию SMTP-трафика**;
- **разрешать исходящий трафик** из локальной сети.

Внутренний межсетевой экран должен принимать входящий трафик только от основного межсетевого экрана и SMTP-сервера.

Наконец, он должен разрешать все исходящие соединения от внутренних систем.

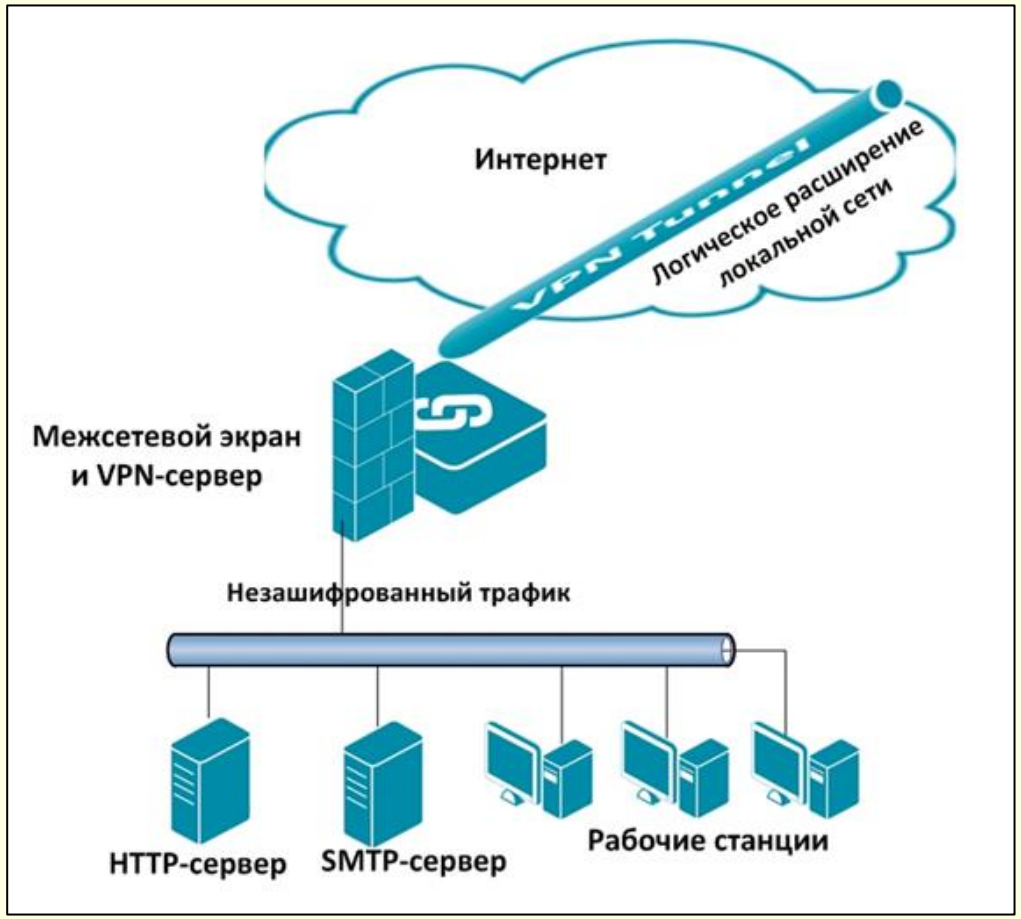
Конфигурация с двумя DMZ-сетями

Чтобы сделать данный пример применимым к окружениям с более высокими требованиями к безопасности, могут быть добавлены следующие сервера и использованы следующие технологии:

- внутренний и внешний DNS-серверы, что обеспечит сокрытие внутренних систем;
- NAT для дальнейшего сокрытия внутренних систем;
- исходящий трафик от внутренних хостов может фильтроваться, что включает фильтрование трафика к определенным сайтам или сервисам в соответствии с политикой управления;

Может быть использовано несколько межсетевых экранов как для увеличения производительности, так и для разграничения трафика между отделами.

Конечные точки VPN



Конечные точки VPN

- Другой функциональностью, которой обычно обладают межсетевые экраны, является возможность функционирования в качестве **конечной точки VPN**.
- VPN создается поверх существующей сетевой среды и протоколов с использованием дополнительных протоколов, обеспечивающих шифрование и целостность трафика.
- VPN применяется для обеспечения безопасных сетевых соединений с использованием сетей, которые не являются доверяемыми.
- Например, технология VPN все чаще создается для **предоставления удаленного доступа пользователя к сетям организации** через интернет.
- Данная технология пользуется возрастающей популярностью, так как это существенно снижает издержки, связанные с возможностью безопасного удаленного доступа, по сравнению с использованием выделенных каналов связи.
- При использовании VPN соединение с интернетом может также использоваться для безопасного удаленного доступа пользователей к сетям и ресурсам организации.

Конечные точки VPN

- С точки зрения используемого протокола, существует несколько возможных выборов для создания VPN.
- Наиболее часто используется семейство протоколов **IPSec** и протокол **L2TP**.
- В большинстве случаев наиболее приемлемым является совмещение конечной точки VPN и межсетевого экрана.
- Как правило, межсетевой экран использует IPSec для соединения с удаленными системами, а к внутренним сетям передает незашифрованный трафик.
- Размещение конечной точки VPN позади межсетевого экрана означает, что VPN-трафик будет передаваться через межсетевой экран в зашифрованном виде, т.е. межсетевой экран не будет иметь возможность анализировать входящий или исходящий VPN-трафик, выполнять управление доступом, создавать логи, сканировать на вирусы и т.п.

Конечные точки VPN

- Однако совмещение межсетевого экрана и конечной точки VPN имеет и свои **негативные стороны**.
- Одним из таких недостатков является **высокая стоимость**.
- Также, так как VPN-трафик должен быть зашифрован, то это существенно уменьшает производительность межсетевого экрана.
- Выполнение шифрования в аппаратуре может существенно увеличить производительность.

Расположение серверов в DMZ-сетях

Где расположить серверы при наличии межсетевых экранов, зависит от многих факторов, включая количество DMZ, необходимость внешнего и внутреннего доступа к серверам, расположенным в DMZ, интенсивность трафика и чувствительность обрабатываемых данных.

Невозможны абсолютно универсальные рекомендации по расположению серверов, но основные принципы должны быть следующими.

- Следует **изолировать серверы** таким образом, чтобы успешные атаки на них не могли причинить ущерба оставшейся части сети, в частности, не следует размещать внешне доступные серверы в защищенной сети.
- Следует **защитить внешне доступные серверы** с помощью пограничного маршрутизатора с возможностями пакетного фильтра.
- Следует **разместить внутренне доступные серверы** в DMZ-сетях, в которых обеспечивается защита как от внешних, так и от внутренних атак, поскольку обычно эти серверы содержат более чувствительные данные и к ним требуется более ограниченный доступ.

Расположение серверов в DMZ-сетях

Внешне доступные серверы

- Внешне доступные HTTP-серверы, а также серверы каталога или DNS-серверы, могут быть размещены во внешней DMZ, т.е. между пограничным маршрутизатором с функциями пакетного фильтра и основным межсетевым экраном.

- Пограничный маршрутизатор может обеспечить некоторое управление доступом и фильтрацию трафика для серверов, а основной межсетевой экран – предотвратить создание соединений от серверов к внутренним системам, которые могут возникнуть, если серверы будут взломаны.

- В случае большого трафика и сильной загруженности серверов может использоваться высокоскоростной пограничный маршрутизатор с несколькими присоединенными DMZ для изолирования серверов в индивидуальных DMZ-сетях.

- Таким образом, если осуществляется DDoS-атака на некоторый сервер, другие сегменты сети не пострадают.

Расположение серверов в DMZ-сетях

VPN- и Dial-in-серверы

- Эти серверы лучше разместить во внешней DMZ, чтобы их трафик проходил в локальную сеть через основной межсетевой экран.
- Одна из возможных конфигураций состоит в совмещении VPN-сервера и межсетевого экрана, чтобы исходящий трафик мог быть зашифрован *после* того, как он будет отфильтрован, и входящий трафик может быть расшифрован и затем отфильтрован межсетевым экраном.
- Dial-in сервер должен быть размещен во внешней DMZ по тем же причинам.

Расположение серверов в DMZ-сетях

Внутренние серверы

- Внутренне доступные HTTP-серверы, SMTP-серверы и серверы каталога могут быть размещены во внутренней DMZ, т.е. между двумя межсетевыми экранами, основным и внутренним; при этом внутренний межсетевой экран отделяет внутреннюю DMZ от защищенной сети.
- Размещение этих систем во внутренней DMZ обеспечивает оборону вглубь, защищая как от внешних, так и от внутренних угроз.
- Если HTTP-прокси используется для исходящего трафика, размещение этих систем во внутренней DMZ обеспечивает большую защиту от внутренних и внешних угроз.

Расположение серверов в DMZ-сетях

DNS-серверы

- Во-первых, **внутренние DNS-серверы должны быть отделены от внешних DNS-серверов**.
- Например, DNS-сервер, который доступен всему миру, не должен содержать записей о системах, которые не должны быть доступны извне.
- Если такие записи о внутренних системах имеются во внешнем DNS-сервере, это даст возможность атакующему определить список целей для атаки.
- Следует поддерживать отдельно внутренний и внешний DNS-серверы либо использовать технологию, известную как ***split DNS***, которая гарантирует, что информация о внутренних системах никогда не будет передана вовне.
- Во-вторых, необходимо установить **разрешенные типы доступа к DNS-серверу**.
- Приложение DNS-сервера может выполняться с использованием двух транспортных протоколов: клиент обращается к серверу по протоколу UDP, а взаимодействие двух серверов DNS, выполняющих зонные пересылки, реализовано с использованием TCP.
- Доступ к серверу DNS с использованием TCP должен быть ограничен только для тех серверов DNS, которые должны выполнять зонные пересылки.

Расположение серверов в DMZ-сетях

- Основной риск, который существует при функционировании DNS, состоит **в модификации передаваемой информации**.
- Например, если сервер допускает неаутентифицированные запросы и ответы DNS, атакующий может модифицировать информацию, в результате чего сетевой трафик будет перенаправлен на другой хост.
- Пример топологии сети с двумя DNS-серверами.
- **Внутренний DNS-сервер** должен быть сконфигурирован для разрешения имен внутренних серверов, чтобы внутренние пользователи могли соединяться с ними, всеми серверами в DMZ и интернетом.
- **Внешний DNS-сервер** должен обеспечивать разрешение имен самого DNS-сервера и серверов во внешней DMZ, но не во внутренней сети.
- Как результат, серверы во внешней DMZ будут видимы в интернете.

Расположение серверов в DMZ-сетях