Обзор вариантов организации доступа к сервисам корпоративной сети из Интернет

© Кившенко Алексей, 1880

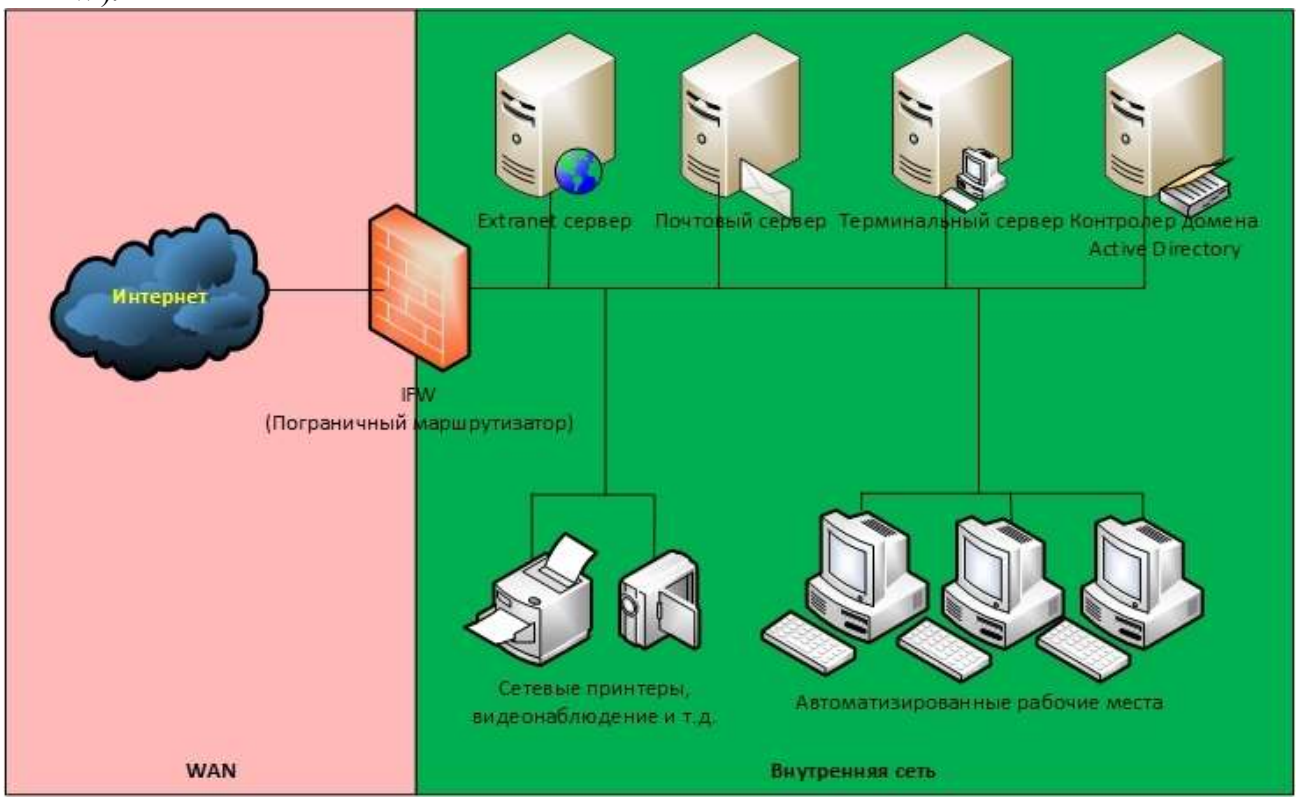
Данная статья содержит обзор *пяти* вариантов решения задачи организации доступа к сервисам корпоративной сети из Интернет. В рамках обзора приводится анализ вариантов на предмет безопасности и реализуемости, что поможет разобраться в сути вопроса, освежить и систематизировать свои знания как начинающим специалистам, так и более опытным. Материалы статьи можно использовать для обоснования Ваших проектных решений.

При рассмотрении вариантов в качестве примера возьмем сеть, в которой требуется опубликовать:

1. Корпоративный почтовый сервер (Web-mail).
2. Корпоративный терминальный сервер (RDP).
3. Extranet сервис для контрагентов (Web-API).

Вариант 1. Плоская сеть

В данном варианте все узлы корпоративной сети содержатся в одной, общей для всех сети («Внутренняя сеть»), в рамках которой коммуникации между ними не ограничиваются. Сеть подключена к Интернет через пограничный маршрутизатор/межсетевой экран (далее — *IFW*).



Доступ узлов в Интернет осуществляется через NAT, а доступ к сервисам из Интернет через Port forwarding.

Плюсы варианта:

1. Минимальные требования к функционалу *IFW* (можно сделать практически на любом, даже домашнем роутере).
2. Минимальные требования к знаниям специалиста, осуществляющего реализацию варианта.

Минусы варианта:

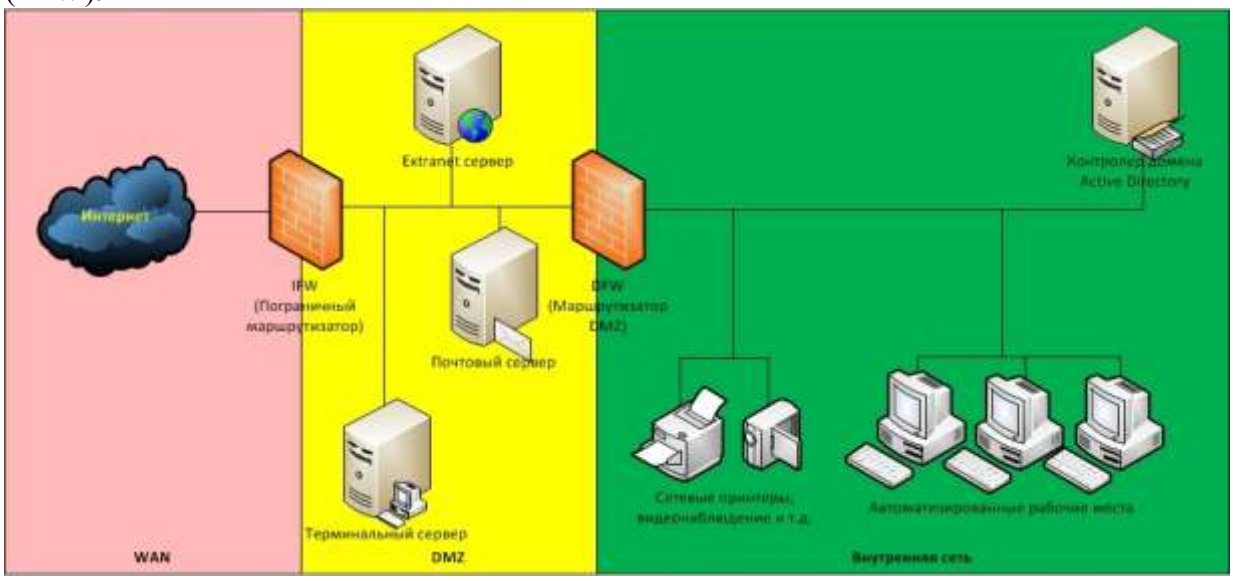
1. Минимальный уровень безопасности. В случае взлома, при котором Нарушитель получит контроль над одним из опубликованных в Интернете серверов, ему для дальнейшей атаки становятся доступны все остальные узлы и каналы связи корпоративной сети.

Аналогия с реальной жизнью
Подобную сеть можно сравнить с компанией, где персонал и клиенты находятся в одной общей комнате (open space)

© *hrmaximum.ru*

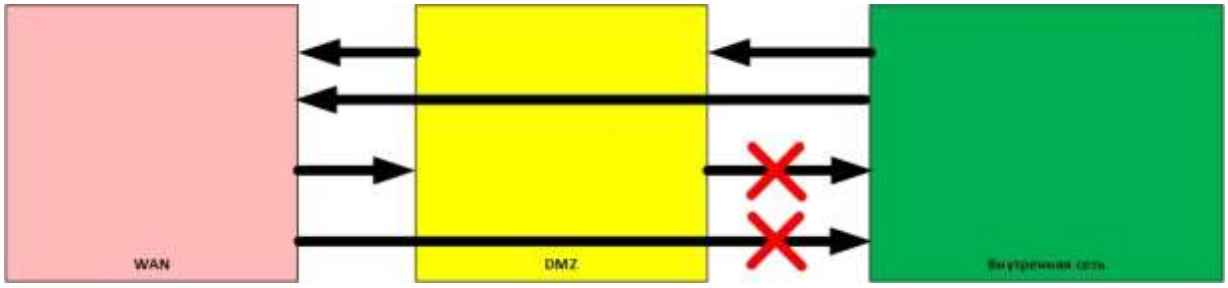
Вариант 2. DMZ

Для устранения указанного ранее недостатка узлы сети, доступные из Интернет, помещают в специально выделенный сегмент – демилитаризованную зону (DMZ). DMZ организуется с помощью межсетевых экранов, отделяющих ее от Интернет (*IFW*) и от внутренней сети (*DFW*).



При этом правила фильтрации межсетевых экранов выглядят следующим образом:

1. Из внутренней сети можно инициировать соединения в DMZ и в WAN (Wide Area Network).
2. Из DMZ можно инициировать соединения в WAN.
3. Из WAN можно инициировать соединения в DMZ.
4. Инициация соединений из WAN и DMZ ко внутренней сети запрещена.



Плюсы варианта:

1. Повышенная защищённость сети от взломов отдельных сервисов. Даже если один из серверов будет взломан, Нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т.д.).

Минусы варианта:

1. Сам по себе вынос серверов в DMZ не повышает их защищенность.
2. Необходим дополнительный МЭ для отделения DMZ от внутренней сети.

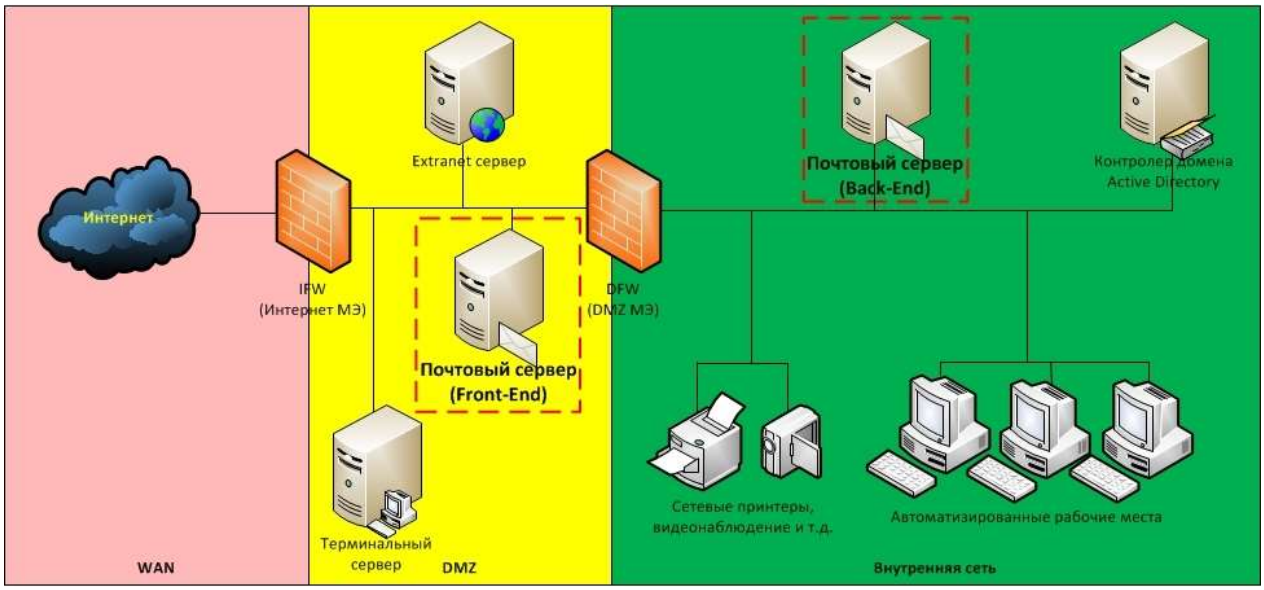
Аналогия с реальной жизнью

Данный вариант архитектуры сети похож на организацию рабочей и клиентской зон в компании, где клиенты могут находиться только в клиентской зоне, а персонал может быть, как в клиентской, так и в рабочих зонах. DMZ сегмент — это как раз и есть аналог клиентской зоны.

© autobam.ru

Вариант 3. Разделение сервисов на Front-End и Back-End

Как уже отмечалось ранее, размещение сервера в DMZ никоим образом не улучшает безопасность самого сервиса. Одним из вариантов исправления ситуации является разделение функционала сервиса на две части: Front-End и Back-End. При этом каждая часть располагается на отдельном сервере, между которыми организуется сетевое взаимодействие. Сервера Front-End, реализующие функционал взаимодействия с клиентами, находящимися в Интернет, размещают в DMZ, а сервера Back-End, реализующие остальной функционал, оставляют во внутренней сети. Для взаимодействия между ними на *DFW* создают правила, разрешающие инициацию подключений от Front-End к Back-End.



В качестве примера рассмотрим корпоративный почтовый сервис, обслуживающий клиентов как изнутри сети, так и из Интернет. Клиенты изнутри используют POP3/SMTP, а клиенты из Интернет работают через Web-интерфейс. Обычно на этапе внедрения компании выбирают наиболее простой способ развертывания сервиса и ставят все его компоненты на один сервер. Затем, по мере осознания необходимости обеспечения информационной безопасности, функционал сервиса разделяют на части, и та часть, что отвечает за обслуживание клиентов из Интернет (Front-End), выносится на отдельный сервер, который по сети взаимодействует с сервером, реализующим оставшийся функционал (Back-End). При этом Front-End размещают в DMZ, а Back-End остается во внутреннем сегменте. Для связи между Front-End и Back-End на *DFW* создают правило, разрешающее, инициацию соединений от Front-End к Back-End.

Плюсы варианта:

1. В общем случае атаки, направленные против защищаемого сервиса, могут «споткнуться» об Front-End, что позволит нейтрализовать или существенно снизить возможный ущерб. Например, атаки типа TCP SYN Flood или slow http read, направленные на сервис, приведут к тому, что Front-End сервер может оказаться

недоступен, в то время как Back-End будет продолжать нормально функционировать и обслуживать пользователей.
2. В общем случае на Back-End сервере может не быть доступа в Интернет, что в случае его взлома (например, локально запущенным вредоносным кодом) затруднит удаленное управление им из Интернет.
3. Front-End хорошо подходит для размещения на нем межсетевого экрана уровня приложений (например, Web application firewall) или системы предотвращения вторжений (IPS, например snort).

Минусы варианта:

1. Для связи между Front-End и Back-End на *DFW* создается правило, разрешающее инициацию соединения из DMZ во внутреннюю сеть, что порождает угрозы, связанные с использованием данного правила со стороны других узлов в DMZ (например, за счет реализации атак IP spoofing, ARP poisoning и т. д.)
2. Не все сервисы могут быть разделены на Front-End и Back-End.
3. В компании должны быть реализованы бизнес-процессы актуализации правил межсетевого экранирования.
4. В компании должны быть реализованы механизмы защиты от атак со стороны Нарушителей, получивших доступ к серверу в DMZ.

Примечания

1. В реальной жизни даже без разделения серверов на Front-End и Back-End серверам из DMZ очень часто необходимо обращаться к серверам, находящимся во внутренней сети, поэтому указанные минусы данного варианта будут также справедливы и для предыдущего рассмотренного варианта.
2. Если рассматривать защиту приложений, работающих через Web-интерфейс, то даже если сервер не поддерживает разнесение функций на Front-End и Back-End, применение http reverse proxy сервера (например, nginx) в качестве Front-End позволит минимизировать риски, связанные с атаками на отказ в обслуживании. Например, атаки типа SYN flood могут сделать http reverse proxy недоступным, в то время как Back-End будет продолжать работать.

Аналогия с реальной жизнью
Данный вариант по сути похож на организацию труда, при которой для высоко загруженных работников используют помощников — секретарей. Тогда Back-End будет аналогом загруженного работника, а Front-End аналогом секретаря.

© *mln.kz*

Вариант 4. Защищенный DMZ

DMZ это часть сети, доступная из Internet, и, как следствие, подверженная максимальному риску компрометации узлов. Дизайн DMZ и применяемые в ней подходы должны обеспечивать максимальную живучесть в условиях, когда Нарушитель получил контроль над одним из узлов в DMZ. В качестве возможных атак рассмотрим атаки, которым подвержены практически все информационные системы, работающие с настройками по умолчанию:

1. CAM-table overflow
2. ARP poisoning
3. Rogue DHCP Server
4. DHCP starvation
5. VLAN hopping
6. MAC flood
7. UDP flood
8. TCP SYN flood
9. TCP session hijacking
10. TCP reset
11. Атаки на Web-приложения
12. Атаки на обход средств аутентификации и авторизацию от имени легитимного пользователя (например, подбор паролей, PSK и т.д.)
13. Атаки на уязвимости в сетевых службах, например:

- Атака на Web-сервер — slow reading
- DNS cache poisoning

Большая часть указанных атак (по крайней мере с 1 по 10) базируется на уязвимостях архитектуры современных Ethernet/IP сетей, заключающихся в возможности Нарушителя

подделывать в сетевых пакетах MAC и IP адреса. Эксплуатацию данных уязвимостей иногда выделяют в отдельный виды атак:

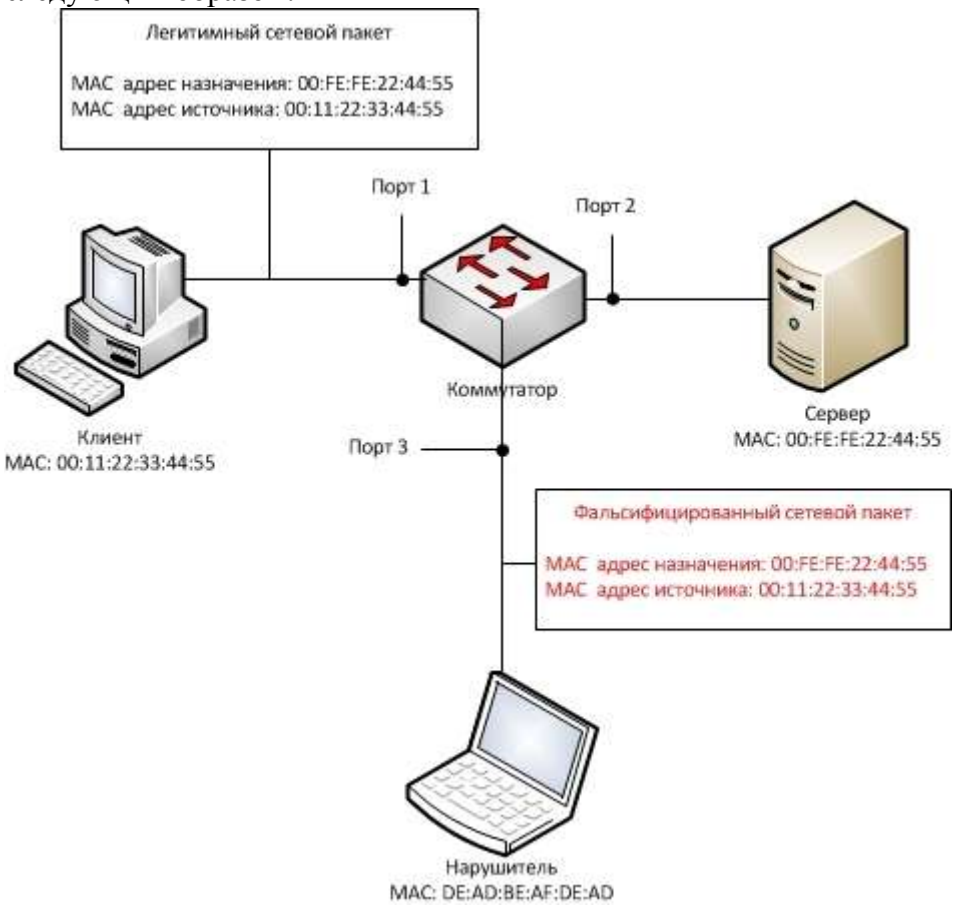
1. MAC spoofing;
2. IP spoofing.

Поэтому построение системы защиты DMZ начнем с рассмотрения способов защиты от IP и MAC spoofing.

Примечание
Приведенные ниже способы защиты от данных атак не являются единственно возможными. Существуют и другие способы.

Защита от MAC spoofing

Схематически атаки, связанные с подменой MAC адреса, можно проиллюстрировать следующим образом:

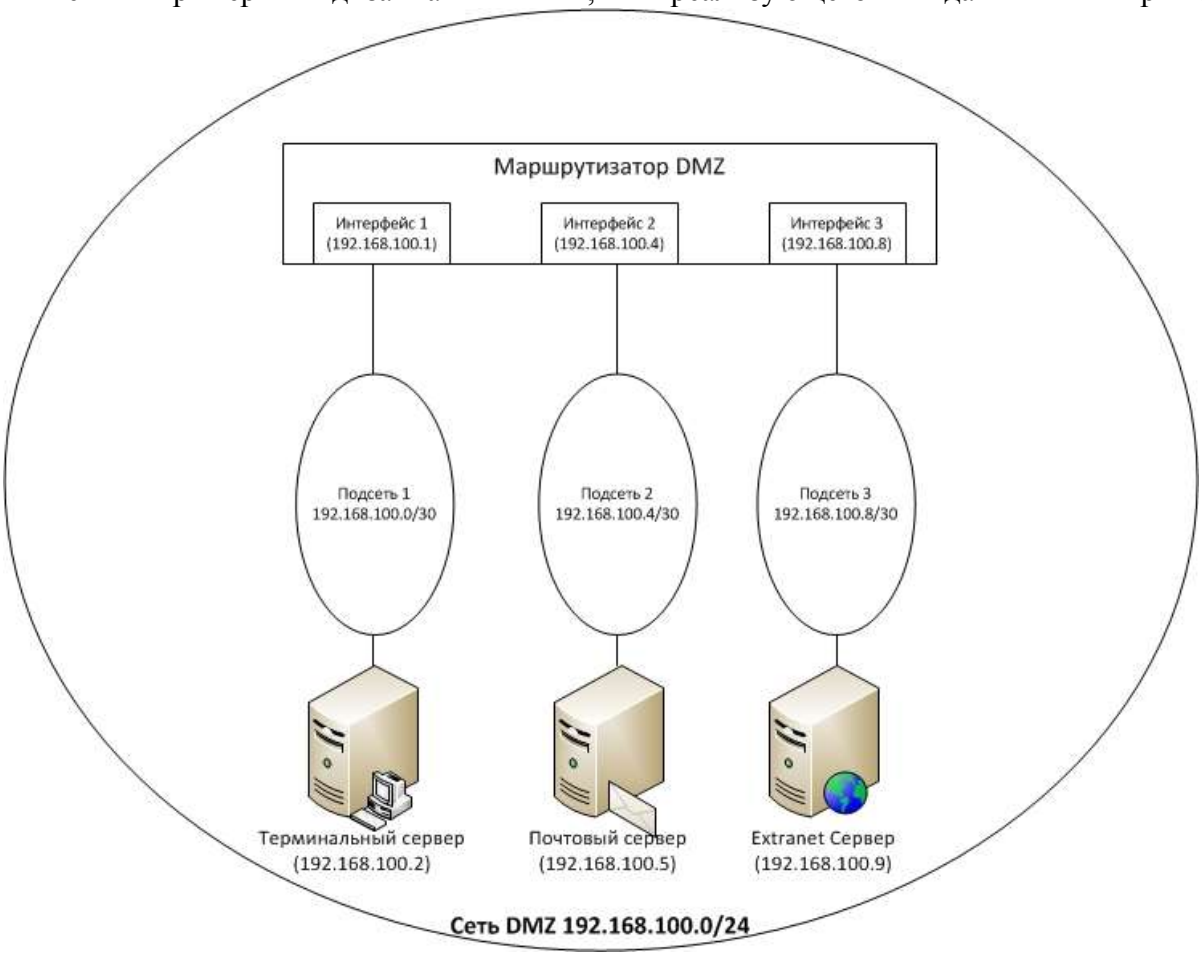


Нейтрализацией данной атаки может являться фильтрация MAC-адресов на портах коммутатора. Например, трафик по порту 3 должен проходить только в случае, если в адресе источника или в адресе назначения указан MAC-адрес DE:AD:BE:AF:DE:AD или широковещательный адрес (в некоторых случаях).

Защита от IP spoofing

Схема атаки IP spoofing похожа на предыдущую, за исключением того, что Нарушитель

подделывает не MAC, а IP-адрес. Защита от IP spoofing может быть реализована путем разделения IP-сети DMZ на более мелкие IP-подсети и дальнейшей фильтрацией трафика на интерфейсах маршрутизатора по аналогии с рассмотренной ранее MAC-фильтрацией. Ниже пример дизайна DMZ, реализующего данный принцип:



В DMZ располагается 3 узла:

- Терминальный сервер (192.168.100.2)
- Почтовый сервер (192.168.100.5)
- Extranet сервер (192.168.100.9)

Для DMZ выделена IP-сеть 192.168.100.0/24, в данной сети выделяются 3 IP-подсети (по числу серверов):
Подсеть 1 — 192.168.100.0/30 для терминального сервера (192.168.100.2)
Подсеть 2 — 192.168.100.4/30 для почтового сервера (192.168.100.5)
Подсеть 3 — 192.168.100.8/30 для почтового сервера (192.168.100.9)

На практике разделение сети на подобные подсети реализуют с помощью технологии VLAN. Однако, ее применение порождает риски, защиту от которых мы сейчас рассмотрим.

Защита от VLAN hopping

Для защиты от этой атаки на коммутаторе отключают возможность автоматического

согласования типов (trunk / access) портов, а сами типы администратор назначает вручную. Кроме того, организационными мерами запрещается использование так называемого native VLAN.

Защита от атак, связанных с DHCP

Несмотря на то, что DHCP предназначен для автоматизации конфигурирования IP-адресов рабочих станций, в некоторых компаниях встречаются случаи, когда через DHCP выдаются IP-адерса для серверов, но это довольно плохая практика. Поэтому для защиты от Rogue DHCP Server, DHCP starvation рекомендуется полный отказ от DHCP в DMZ.

Защита от атак MAC flood

Для защиты от MAC flood проводят настройку на портах коммутатора на предмет ограничения предельной интенсивности широковещательного трафика (поскольку обычно при данных атаках генерируется широковещательный трафик (broadcast)). Атаки, связанные с использованием конкретных (unicast) сетевых адресов, будут заблокированы MAC фильтрацией, которую мы рассмотрели ранее.

Защита от атак UDP flood

Защита от данного типа атак производится аналогично защите от MAC flood, за исключением того, что фильтрация осуществляется на уровне IP (L3).

Защита от атак TCP SYN flood

Для защиты от данной атаки возможны варианты:

1. Защита на узле сети с помощью технологии TCP SYN Cookie.
2. Защита на уровне межсетевого экрана (при условии разделения DMZ на подсети) путем ограничения интенсивности трафика, содержащего запросы TCP SYN.

Защита от атак на сетевые службы и Web-приложения

Универсального решения данной проблемы нет, но устоявшейся практикой является внедрение процессов управления уязвимостями ПО (выявление, установка патчей и т.д., например, так), а также использование систем обнаружения и предотвращения вторжений (IDS/IPS).

Защита от атак на обход средств аутентификации

Как и для предыдущего случая универсального решения данной проблемы нет. Обычно в случае большого числа неудачных попыток авторизации учетные записи, для

избежания подборов аутентификационных данных (например, пароля) блокируют. Но подобный подход довольно спорный, и вот почему.
Во-первых, Нарушитель может проводить подбор аутентификационной информации с интенсивностью, не приводящей к блокировке учетных записей (встречаются случаи, когда пароль подбирался в течении нескольких месяцев с интервалом между попытками в несколько десятков минут).

Во-вторых, данную особенность можно использовать для атак типа отказ в обслуживании, при которых Нарушитель будет умышленно проводить большое количество попыток авторизации для того, чтобы заблокировать учетные записи.
Наиболее эффективным вариантом от атак данного класса будет использование систем IDS/IPS, которые при обнаружении попыток подбора паролей будут блокировать не учетную запись, а источник, откуда данный подбор происходит (например, блокировать IP-адрес Нарушителя).

Итоговый перечень защитных мер по данному варианту:

1. DMZ разделяется на IP-подсети из расчета отдельная подсеть для каждого узла.
2. IP адреса назначаются вручную администраторами. DHCP не используется.
3. На сетевых интерфейсах, к которым подключены узлы DMZ, активируется MAC и IP фильтрация, ограничения по интенсивности широковещательного трафика и трафика, содержащего TCP SYN запросы.
4. На коммутаторах отключается автоматическое согласование типов портов, запрещается использование native VLAN.
5. На узлах DMZ и серверах внутренней сети, к которым данные узлы подключаются, настраивается TCP SYN Cookie.
6. В отношении узлов DMZ (и желательно остальной сети) внедряется управление уязвимостями ПО.
7. В DMZ-сегменте внедряются системы обнаружения и предотвращения вторжений IDS/IPS.

Плюсы варианта:

1. Высокая степень безопасности.

Минусы варианта:

1. Повышенные требования к функциональным возможностям оборудования.
2. Трудозатраты во внедрении и поддержке.

Аналогия с реальной жизнью
Если ранее DMZ мы сравнили с клиентской зоной, оснащенной диванчиками и пуфиками, то защищенный DMZ будет больше похож на бронированную кассу.

© *valmax.com.ua*

Вариант 5. Back connect

Рассмотренные в предыдущем варианте меры защиты были основаны на том, что в сети присутствовало устройство (коммутатор / маршрутизатор / межсетевой экран), способное их реализовывать. Но на практике, например, при использовании виртуальной инфраструктуры (виртуальные коммутаторы зачастую имеют очень ограниченные возможности), подобного устройства может и не быть.

В этих условиях Нарушителю становятся доступны многие из рассмотренных ранее атак, наиболее опасными из которых будут:

- атаки, позволяющие перехватывать и модифицировать трафик (ARP Poisoning, CAM table overflow + TCP session hijacking и др.);
- атаки, связанные с эксплуатацией уязвимостей серверов внутренней сети, к которым можно инициировать подключения из DMZ (что возможно путем обхода правил фильтрации *DFW* за счет IP и MAC spoofing).

Следующей немаловажной особенностью, которую мы ранее не рассматривали, но которая не перестает быть от этого менее важной, это то, что автоматизированные рабочие места (АРМ) пользователей тоже могут быть источником (например, при заражении вирусами или троянами) вредоносного воздействия на сервера.

Таким образом, перед нами встает задача защитить сервера внутренней сети от атак Нарушителя как из DMZ, так и из внутренней сети (заражение АРМа трояном можно интерпретировать как действия Нарушителя из внутренней сети).

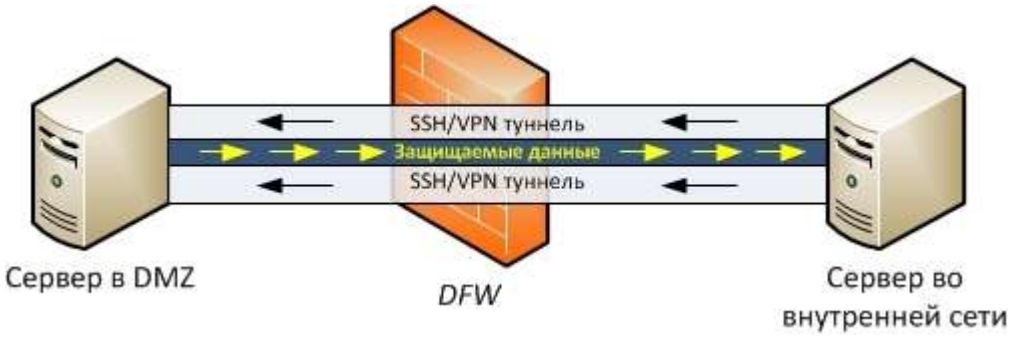
Предлагаемый далее подход направлен на уменьшение числа каналов, через которые Нарушитель может атаковать сервера, а таких канала как минимум два. Первый это правило на *DFW*, разрешающее доступ к серверу внутренней сети из DMZ (пусть даже и с ограничением по IP-адресам), а второй — это открытый на сервере сетевой порт, по которому ожидаются запросы на подключение.

Закрыть указанные каналы можно, если сервер внутренней сети будет сам строить соединения до сервера в DMZ и будет делать это с помощью криптографически защищенных сетевых протоколов. Тогда не будет ни открытого порта, ни правила на *DFW*.

Но проблема в том, что обычные серверные службы не умеют работать подобным образом, и для реализации указанного подхода необходимо применять сетевое туннелирование, реализованное, например, с помощью SSH или VPN, а уже в рамках туннелей разрешать подключения от сервера в DMZ к серверу внутренней сети.

Общая схема работы данного варианта выглядит следующим образом:

1. На сервер в DMZ инсталлируется SSH/VPN сервер, а на сервер во внутренней сети инсталлируется SSH/VPN клиент.
2. Сервер внутренней сети инициирует построение сетевого туннеля до сервера в DMZ. Туннель строится с взаимной аутентификацией клиента и сервера.
3. Сервер из DMZ в рамках построенного туннеля инициирует соединение до сервера во внутренней сети, по которому передаются защищаемые данные.
4. На сервере внутренней сети настраивается локальный межсетевой экран, фильтрующий трафик, проходящий по туннелю.



Использование данного варианта на практике показало, что сетевые туннели удобно строить с помощью OpenVPN, поскольку он обладает следующими важными свойствами:

- Кроссплатформенность. Можно организовывать связь на серверах с разными операционными системами.
- Возможность построения туннелей с взаимной аутентификацией клиента и сервера.
- Возможность использования сертифицированной криптографии.

На первый взгляд может показаться, что данная схема излишне усложнена и что, раз на сервере внутренней сети все равно нужно устанавливать локальный межсетевой экран, то проще сделать, чтобы сервер из DMZ, как обычно, сам подключался к серверу внутренней сети, но делал это по шифрованному соединению. Действительно, данный вариант закроет много проблем, но он не сможет обеспечить главного — защиту от атак на уязвимости

сервера внутренней сети, совершаемых за счет обхода межсетевого экрана с помощью IP и MAC spoofing.

Плюсы варианта:

1. Архитектурное уменьшение количества векторов атак на защищаемый сервер внутренней сети.
2. Обеспечение безопасности в условиях отсутствия фильтрации сетевого трафика.
3. Защита данных, передаваемых по сети, от несанкционированного просмотра и изменения.
4. Возможность избирательного повышения уровня безопасности сервисов.
5. Возможность реализации двухконтурной системы защиты, где первый контур обеспечивается с помощью межсетевого экранирования, а второй организуется на базе данного варианта.

Минусы варианта:

1. Внедрение и сопровождение данного варианта защиты требует дополнительных трудовых затрат.
2. Несовместимость с сетевыми системами обнаружения и предотвращения вторжений (IDS/IPS).
3. Дополнительная вычислительная нагрузка на сервера.

Аналогия с реальной жизнью
Основной смысл данного варианта в том, что доверенное лицо устанавливает связь с не доверенным, что похоже на ситуацию, когда при выдаче кредитов Банки сами перезванивают потенциальному заемщику с целью проверки данных.

© comfoson.890m.com

Заключение

Итак, мы рассмотрели все пять заявленных вариантов организации доступа к сервисам корпоративной сети из Интернет. Какой из них лучше, какой хуже — сказать сложно, поскольку все зависит, в конечном счете, от той информации, которую необходимо защитить, и тех ресурсов, которыми компания располагает для защиты. Если ни ресурсов, ни знаний нет, то оптимальным будет первый вариант. Если же информация очень ценна, то комбинация четвертого и пятого вариантов даст непревзойденный уровень безопасности.