Выделение адресов для частных подсетей интернета

Содержание

Введение

Этот документ основан на RFC 1597, и это поможет вам сохранять пространство IP-адресов, не выделяя глобально уникальные IP - адреса закрытым хостам в вашей сети. По-прежнему можно разрешить полное подключение сетевого уровня между всеми хостами сети и всеми общими хостами Интернета.

Узлы, использующие IP, делятся на три категории:

- Хосты, которые не требуют доступа к хостам на других предприятиях или Интернете в целом. Эти хосты могут использовать IP-адреса, которые уникальны в пределах своей сети, но за ее пределами могут таковыми не быть.
- Хосты, для которых требуется доступ к ограниченному набору внешних служб (например электронная почта, FTP, сетевые новости, удаленный вход), которые могут обслуживаться шлюзами уровня приложения. Многим из этих хостов из соображений конфиденциальности и безопасности не нужен неограниченный внешний доступ (предоставленный через IP-соединение). Так же, так и узлы в первой категории, они могут использовать IP-адреса, уникальные в их сети, но не среди внешних сетей.
- Хосты, которым нужен доступ на уровне сети за пределами предприятия, предоставленного через возможность подключения с помощью IP-адреса. Только эти хосты требуют IP-адресов, которые глобально уникальны.

Много приложений требуют подключения только в одной сети и даже не нужны в возможности внешних подключений для большинства внутренних хостов. В больших сетях узлы часто используют TCP/IP, когда им не требуется подключение сетевого уровня за пределами сети. Вот некоторые примеры, где не могла бы требоваться возможность внешних подключений:

- Большой аэропорт, в котором есть экраны прибытия и вылета, имеет отдельный адрес посредством TCP/IP. Маловероятно, что для этих электронных табло требуется доступ из других сетей.
- Большие компании, например банки или сети розничных магазинов, использующие TCP/IP для обеспечения внутренней связи. Большим числам локальных рабочих станций как кассы, денежных машин и оборудования в конторских позициях редко нужно внешнее подключение.
- Сети, которые используют шлюзы уровня приложения (межсетевые экраны) для соединения с Интернетом. Внутренняя сеть обычно не имеет прямого доступа к Интернету, таким образом, только один или несколько хостов межсетевого экрана видимы из Интернета. В этом случае внутренняя сеть может использовать групповые IP-адреса.
- Две сети, связанные по частному каналу. Обычно только очень ограниченный набор хостов взаимно достижим по этой ссылке. Только для этих хостов требуются глобально уникальные IP-номера.
- Интерфейсы маршрутизаторов на внутренней сети.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Частное адресное пространство

Комитет по цифровым адресам в интернете (IANA) резервировал следующие три блока пространства IP-адресов для частных сетей:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Первый блок является номером отдельной сети класса A, второй блок – набор их 16 номеров смежной сети класса B, третий блок – набор из 255 номеров смежной сети класса C.

Если принято решение использовать частное пространство адресов, то согласование с IANA или Интернет-реестром не нужно. Адреса этого частного адресного пространства

будут уникальными только в пределах вашей сети. Следует помнить, что если необходимо глобальное уникальное адресное пространство, то понадобится приобрести адреса из реестра Интернета.

Чтобы использовать частное адресное пространство, определите, каким узлам не требуется внешнее подключение сетевого уровня. Данные хосты являются частными и используют частное адресное пространство. Закрытые хосты могут связаться со всеми другими хостами в сети, и общественной и частной, но у них не может быть возможности подключения с помощью IP-адреса ни к какому внешнему хосту. Закрытые хосты все еще могут получать доступ к внешним службам через ретрансляцию на уровне приложений.

Все остальные хосты являются открытыми и используют пространство глобально уникальных адресов, назначенное службой регистрации абонентов Интернета. Открытые хосты могут взаимодействовать с другими хостами сети и подключаться через IP к внешним открытым хостам. Соединение между открытыми и частными хостами в других сетях отсутствует.

Поскольку частные адреса не имеют никакого глобального значения, сведения о маршрутизации о частных сетях не распространяются на внешних каналах, и пакеты с частными адресами источника или назначения не должны быть переданы через такие ссылки. Маршрутизаторы в сетях, не использующих частное пространство адресов, особенно сети поставщиков Интернет-услуг, должны быть настроены на отклонение (фильтрацию) маршрутной информации о частных сетях. Это отклонение не должно рассматриваться как ошибка протокола маршрутизации.

Непрямые ссылки на данные адреса (например, ресурсные записи DNS) должны храниться в пределах сети. Поставщики Интернет-услуг должны принимать меры для предотвращения такой утечки.

Достоинства и недостатки использования частного адресного пространства

Очевидное преимущество использования частного пространства адресов для Интернета в целом должно сохранить глобально уникальное пространство адресов. Использование пространства частных адресов дает вам возможность более гибко проектировать сеть, поскольку в этом случае в вашем распоряжении будет больше адресов, чем при использовании адресов из глобально уникального пула.

Основной недостаток использования частного пространства адресов заключается в том, что приходится изменять порядок IP-адресов, если необходимо подключиться к сети Internet.

Принципы проектирования

Необходимо разработать личную часть сети сначала и использовать частное пространство адресов для всех внутренних ссылок. Затем спланируйте открытую подсеть и разработайте схему внешнего подключения.

Если подходящая схема подсетей может быть разработана и поддерживается вашим оборудованием, используйте 24-разрядный блок частного пространства адресов и сделайте план адресации с хорошим путем роста. Если использование подсетей вызывает проблемы,

можно использовать 16-битный блок класса C.

Изменение хоста с закрытого на общедоступный требует изменения его адреса и, в большинстве случаев, его физического соединения. Можно настроить отдельные физические носители для открытых и закрытых подсетей в местах, где можно предвидеть подобные изменения (компьютерные залы и т.п.), чтобы упростить эти изменения.

Маршрутизаторы, подключающиеся к внешним сетям, должны во избежание утечки устанавливать соответствующие фильтры пакетов и маршрутов на обоих концах канала. Также следует отфильтровывать входящие сведения о маршрутизации, поступающие в любые частные сети, чтобы предотвратить возникновение спорных ситуаций; они могут возникнуть, если маршруты частного пространства адресов ведут за пределы сети.

Группа организаций, которым требуется поддерживать связь между собой, может разработать общий план адресации. Если требуется соединить два узла с помощью внешнего поставщика услуг, можно рассмотреть возможность использования IP-туннеля для предотвращения утечек пакетов из частной сети.

Один из способов избежать утечки записей DNS RR состоит в следующем: запустите два сервера имен, один внешний сервер, отвечающий за все глобально уникальные IP-адреса сети предприятия, и один внутренний сервер, отвечающий за все IP-адрес - как общедоступные, так и частные. Для обеспечения непротиворечивости, оба этих сервера должны получить те же данные, которых внешний сервер имен только использует фильтруемую версию.

Преобразователи на всех внешних хостах (общих и частных) посылают запрос только на внешний сервер имен. Внешний сервер разрешает запросы от внешних преобразователей и подключается к глобальной DNS. Внутренний сервер вперед все запросы для получения информации за пределами предприятия к внешнему серверу имен, таким образом, все внутренние хосты могут обратиться к глобальному DNS. Таким образом, сведения о частных хостах не поступают к внешним преобразователям и именованным серверам.

Вопросы обеспечения безопасности

Хотя использование частного адресного пространства может повысить эффективность защиты, его нельзя считать заменой специальным мерам безопасности.

Заключение

Благодаря данной схеме многим крупным сетям требуется лишь небольшой блок адресов из глобально уникального пространства IP-адресов. Интернет в полной мере пользуется преимуществом сохранения глобально уникального адресного пространства, а сети – преимуществом более высокой гибкости благодаря относительно широкому частному адресному пространству.

Дополнительные сведения

- Протоколы маршрутизируемые по IP
- Страница поддержки IP-маршрутизации
- Cisco Systems – техническая поддержка и документация