

Обеспечение безопасности сетей с использованием частных виртуальных локальных сетей (VLAN) и списков контроля доступа

Содержание

[Введение](#)

[Перед началом работы](#)

[Условные обозначения](#)

[Предварительные условия](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Важность принудительного включения правильной модели доверия](#)

[Частные сети VLAN](#)

[Списки управления доступом VLAN](#)

[Известные ограничения VACL и PVLAN](#)

[Наглядные примеры](#)

[Транзит через демилитаризованную зону](#)

[Внешняя безопасная зона](#)

[Концентратор VPN параллельно с межсетевым экраном](#)

[Дополнительные сведения](#)

[Введение](#)

Одним из ключевых факторов для создания успешного проекта безопасности сети является определение и применение правильной модели доверия. Правильная модель доверия определяет объекты общения и типы передаваемого трафика; остальной трафик отклоняется. Как только идентифицирована правильная трастовая модель, разработчик средств безопасности должен решить, как укрепить модель. С большей глобальной доступностью критичных ресурсов и появлением новых видов сетевых атак инфраструктура сетевой безопасности становится более сложной и появляется больше продуктов для обеспечения безопасности. Такие продукты и технологии как межсетевые экраны, маршрутизаторы, коммутаторы локальных сетей LAN, системы защиты от несанкционированного доступа, серверы AAA и виртуальные частные сети VPN помогают реализовать модель доверия. Разумеется, каждый из подобных продуктов играет особую роль в использовании общих систем защиты. И разработчику важно понимать, как применяются все ее элементы.

[Перед началом работы](#)

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Предварительные условия

В этом документе описаны конфигурации PVLAN на коммутаторах, работающих только с CatOS. [Дополнительные сравнительные примеры конфигурации сетей PVLAN для коммутаторов под управлением Cisco IOS и CatOS см. в документе "Конфигурация изолированных частных сетей VLAN для коммутаторов Catalyst".](#)

Не все коммутаторы и версии программного обеспечения поддерживают частные виртуальные локальные сети. [О возможностях поддержки платформ и версий программного обеспечения сетями PVLAN см. в статье Матрица поддержки частных VLAN коммутатором Catalyst.](#)

Используемые компоненты

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

Общие сведения

Определение и применение правильной модели доверия казалось основной задачей. Но после нескольких лет поддержки использования систем безопасности опыт показывает, что проблемы возникают из-за некачественного проектирования системы безопасности. Обычно некачественные разработки являются прямым следствием того, что надлежащая модель доверия не включена принудительно. Это происходит по разным причинам: иногда из-за нечеткого понимания необходимых действий, а иногда из-за того, что применяемые технологии не полностью освоены либо неправильно используются.

В документе приведены подробные сведения о двух функциях, доступных в коммутаторах Catalyst: частных виртуальных локальных сетях (PVLAN) и списках управления доступом сетей (VACLs). Применение этих функций гарантирует адекватную модель доверия как в корпоративной среде, так и в среде провайдера услуг.

Важность принудительного включения правильной модели доверия

Если не принудительно не включить адекватную модель доверия, это немедленно приведет к снижению сопротивляемости всего механизма безопасности вредоносным действиям. Демилитаризованные зоны (DMZ) обычно внедряются без применения политик прав, т.е. способствуют деятельности потенциальных злоумышленников. В этом разделе приводится анализ частоты применения DMZ и последствий некачественного проектирования. Здесь также объясняется, как ограничить, а лучше избежать некоторых этих последствий.

Обычно серверы DMZ только обрабатывают входящие запросы из Интернета и через определенное время иницируют подключение к внутренним серверам (таким как сервер базы данных), находящимся во внутреннем или другом сегменте DMZ. В то же время не

предполагаются переговоры DMZ серверов друг с другом или инициирование подключений к внешнему миру. Таким образом, необходимые потоки трафика описываются с использованием простой модели доверия. Однако зачастую этот тип модели применяется неадекватно.

Проектировщики обычно хотят применить DMZ с помощью общего сегмента для всех серверов без управления трафиком между ними. Например, все серверы находятся в общей сети VLAN. Поскольку внутри той же самой VLAN трафик не контролируется, то если на один из серверов проник злоумышленник, этот сервер может быть использован в качестве источника атаки на любой из серверов и узлов в том же сегменте. Это облегчает деятельность потенциального злоумышленника во время проверки перенаправления порта или атаки на прикладном уровне.

Обычно для управления входящими соединениями используются межсетевые экраны и фильтры пакетов, но ограничение соединений, иницируемых из DMZ, не применяется. Не так давно существовали известные уязвимости в сценарии cgi-bin: злоумышленник мог запустить сеанс X-term, просто отправив поток данных HTTP; это трафик, который должен быть разрешен межсетевым экраном. Если злоумышленник был достаточно удачлив, он мог использовать еще один способ для получения корневого приглашения, обычно какую-либо атаку с переполнением буфера. В большинстве случаев подобного рода проблем можно избежать путем принудительного включения правильной модели доверия. Во-первых, не предполагаются переговоры серверов друг с другом, и во-вторых, никакие соединения не должны исходить от этих серверов к внешнему миру.

Одни и те же комментарии применимы ко многим другим сценариям, начиная от обычных ненадежных сегментов и заканчивая серверными фермами поставщиков услуг доступа к приложениям.

Сети PVLAN и списки VACL в коммутаторах Catalyst помогают определить правильную модель доверия. Сети PVLAN содействуют путем ограничения трафика между хостами в общем сегменте, тогда как сети VACL обеспечивают дальнейший контроль потока трафика, созданного или предназначенного определенному сегменту. Эти средства обсуждены в следующих разделах.

Частные сети VLAN

Сети PVLAN доступны для Catalyst 6000 под управлением CatOS версии 5.4 или более поздней, Catalyst 4000, 2980G, 2980G-A, 2948G и 4912G под управлением CatOS версии 6.2 или более поздней.

С нашей точки зрения сети PVLAN являются инструментом, способствующим разделению трафика на уровне 2 (L2) за счет превращения широкоэвещательного сегмента в нешироковещательный сегмент с множественным доступом. Трафик, приходящий на коммутатор из смешанного порта (то есть порта, который может пересылать и в основные, и во вторичные VLAN), может выходить на все порты, принадлежащие той же основной VLAN. Трафик, приходящий на коммутатор из порта, соответствующего вторичной VLAN (это может быть изолированная сеть, сообщество или двунаправленная VLAN сообщества) может быть направлен на случайный порт или порт, принадлежащий тому же сообществу VLAN. Несколько портов, сопоставляемых с одной изолированной VLAN, не могут обмениваться трафиком.

На следующем рисунке отображена данная концепция.

Рисунок 1: Частные сети VLAN

Первичные сети VLAN представлены голубым цветом; вторичные – красным и желтым. Хост 1 подключен к порту коммутатора, принадлежащему ко вторичной (красной) сети VLAN. Хост 2 подключен к порту коммутатора, принадлежащего желтой вторичной VLAN.

Когда хост выполняет передачу, трафик переносится во вторичной VLAN. Например, когда хост 2 передает трафик, он идет по желтой сети VLAN. Когда хосты принимают трафик, он идет из первичной (голубой) сети VLAN.

Порты с соединенными маршрутизаторами и межсетевыми экранами называются смешанными, так как они способны пересылать трафик по вторичной сети VLAN, обозначенной на схеме как первичная VLAN. Порты, соединенные с каждым из хостов, способны пересылать трафик как из первичной, так и из вторичной сети VLAN, настроенной на этот порт.

На рисунке представлены частные VLAN как разные магистрали, соединяющие маршрутизаторы и хосты: магистраль, связывающая все остальные сети VLAN, является первичной VLAN (голубой), а трафик по голубым сетям VLAN передается из маршрутизаторов в хосты. Внутренние магистрали первичной сети VLAN являются вторичными VLAN, а трафик в них передается из хостов к маршрутизатору.

Как показано на рисунке, первичная сеть VLAN может объединять одну или несколько подчиненных сетей VLAN.

Ранее в настоящем документе было упомянуто, что сети PVLAN содействуют продвижению соответствующей модели доверия путем обеспечения сегрегации хоста в рамках общего сегмента. Теперь, больше узнав о частных VLAN, рассмотрим, как это можно реализовать в нашем начальном сценарии DMZ. Предполагается, что серверы не общаются друг с другом, но им, тем не менее, необходимо обмениваться данными с межсетевым экраном или маршрутизатором, с которым они соединены. В данном случае серверы должны быть подключены к изолированным портам, а маршрутизаторы и межсетевые экраны подключены к портам, работающим в режиме приема всех пакетов. Таким образом, если один из серверов скомпрометирован, злоумышленник не сможет использовать его в качестве источника атаки на другой сервер в том же сегменте. Коммутатор отбросит любой пакет, передаваемый со скоростью проводной передачи без нарушения производительности.

Еще одно важное замечание: контроль такого типа можно применить только к устройствам L2, так как все серверы принадлежат одной подсети. Брандмауэр или маршрутизатор никак не могут на это повлиять, поскольку серверы будут пытаться связаться напрямую. Кроме того, можно установить порт межсетевого экрана для каждого сервера, но это, скорее всего, не масштабируется и будет слишком сложно и дорого.

В последующем разделе подробно описаны типичные сценарии использования данной функции.

[Списки управления доступом VLAN](#)

VACL доступны в коммутаторах Catalyst серии 6000 под управлением CatOS 5.3 или более поздних версий.

VACL можно настроить на Catalyst 6500 на уровне L2 без необходимости в маршрутизаторе (требуется лишь карта Policy Feature Card (PFC)). Эти функции применяются на скорости проводной передачи (без нарушения производительности) при настройке списков VACL в маршрутизаторе Catalyst 6500. Поскольку поиск списков VACL выполняется на аппаратном уровне вне зависимости от размера списка доступа, скорость пересылки остается неизменной.

Списки VACL могут сопоставляться отдельно в первичной или вторичной сетях VLAN. Настройка списков VACL во вторичных VLAN позволяет фильтровать трафик, генерируемый хостами, не затрагивая трафик между маршрутизаторами и межсетевыми экранами.

Путем объединения списков VACL и частных сетей VLAN возможно фильтровать трафик на основе его направления (передачи). Так, если два маршрутизатора подключены к тому же сегменту, что и некоторые хосты (например, серверы), можно настроить списки VACL во вторичных VLAN так, чтобы фильтровать только трафик, генерируемый хостами, не затрагивая трафик обмена данными между маршрутизаторами.

Для применения соответствующей модели доверия могут быть развернуты VACL. Рассмотрим пример демилитаризованной зоны (DMZ). Предполагается, что серверы DMZ работают только с входящими соединениями, они не запускают соединения во вне. Для управления исходящим трафиком данных серверов к вторичным сетям VLAN может быть применен список VACL. Важно отметить, что при использовании VACL трафик отбрасывается на аппаратном уровне, поэтому никакого воздействия ни на CPU маршрутизатора, ни на CPU коммутатора не оказывается. В случае, если один из серверов окажется источником атаки распределенного отказа от обслуживания (DDoS), коммутатор сбросит незаконный трафик со скоростью проводной передачи без нарушения производительности. Похожие фильтры применяются в маршрутизаторах или межсетевых экранах, присоединенных к серверам, но обычно это имеет серьезные последствия, связанные с производительностью.

На основе MAC ACL не работают хорошо с IP - трафиком, таким образом, VACL рекомендуют контролировать / PVLAN дорожки.

Известные ограничения VACL и PVLAN

При настройке фильтрации с VACL будьте осторожны с обработкой фрагментов на PFC, а также с настройкой в соответствии со спецификацией оборудования.

Учитывая конструктивные особенности PFC модуля Supervisor 1 в Catalyst 6500, лучше всего в явной форме запретить фрагменты ICMP. Причиной является то, что фрагменты протокола ICMP и эхо-ответ воспринимаются аппаратным обеспечением одинаково и по умолчанию аппаратное обеспечение программируется на явное разрешение фрагментов. **Поэтому, если необходимо остановить пакеты эхо-ответа от сервера, необходимо в явном виде указать это с помощью команды `deny icmp any any fragment`.** В конфигурациях, описанных в данном документе, эти особенности принимаются во внимание.

Существует известное ограничение безопасности для PVLAN: возможность того, что маршрутизатор перенаправит трафик обратно в ту же подсеть, из которой он пришел. Маршрутизатор может распределять трафик через изолированные порты, отменяя назначение PVLAN. Это ограничение обусловлено тем, что PVLAN являются средством, которое предоставляет изоляцию на уровне 2 (L2), а не на уровне 3 (L3).

Одноадресный обратный путь пересылки (uRPF) плохо сочетается с портами хостов сети PVLAN, поэтому uRPF с данной сетью не используется.

Эта проблема устраняется путем настройки списков VACL в первичных сетях VLAN. В этом исследовании описаны VACL, которые нужно создать в основной VLAN для сброса трафика, вышедшего из одной подсети и направленного обратно в нее же.

На некоторых картах предусмотрены определенные ограничения по конфигурации сопоставления, карт и магистральных портов PVLAN, например, конфигурация нескольких сопоставлений PVLAN возможна, только если они принадлежат специализированным интегральным схемам (ASIC) с различными портами. Эти ограничения переносятся на новый порт ASIC Coi3. Дополнительные сведения об этом содержатся в последней версии документации к коммутаторам Catalyst по настройке ПО.

Наглядные примеры

В приведенном ниже разделе содержатся три практических примера, которые, по нашему мнению, описывают большинство внедрений и предоставляют подробную информацию о безопасном развертывании PVLAN и VACL.

Эти сценарии выглядят следующим образом:

- Транзит через демилитаризованную зону
- Внешняя безопасная зона
- Концентратор VPN параллельно с межсетевым экраном

Транзит через демилитаризованную зону

Это один из наиболее распространенных сценариев. В данном примере демилитаризованная зона (DMZ) реализована в виде транзитной зоны между двумя маршрутизаторами межсетевого экрана, как показано ниже.

Рис. 2: Транзит через демилитаризованную зону

В данном примере предполагается, что доступ к серверам DMZ имеют как внешние, так и внутренние пользователи. При этом у них нет необходимости общаться друг с другом. В некоторых случаях серверам DMZ требуется разрывать некоторый вид подключений к внутреннему узлу. В то же время предполагается, что внутренние клиенты имеют доступ к Интернету без ограничений. Это хорошо видно на следующем примере. Веб-серверам в DMZ необходимо взаимодействовать с сервером базы данных, расположенной во внутренней сети и имеющей внутренних клиентов с доступом в Интернет.

Внешний межсетевой экран настроен на разрешение входящих подключений к серверам, расположенным в DMZ, но обычно на исходящий трафик наложены ограничения или фильтры, в частности на трафик от DNZ. чения или фильтры, в частоили фильтры, в частолагодаря уменьшккоманыоперации в регулярные интервалы. 0. Как говорилось ранее в этом документе, существуют две потенциальные причины, облегчающие деятельность злоумышленника: первая причина состоит в том, что как только в одном из хостов DMZ обнаружено проникновение, все остальные хосты DMZ также уязвимы. Вторая причина: злоумышленник может легко использовать любое исходящее соединение.

Теперь, когда нет необходимости взаимодействия серверов DMZ друг с другом, необходимо убедиться, что они изолированы на уровне 2 L2. Порты серверов сетей PVLAN называются изолированными, а порты, соединяющие два межсетевых экрана – смешанными. Это достигается определением первичной локальной сети (VLAN) для межсетевых экранов и вторичной сети VLAN для серверов DMZ.

Для управления трафиком, созданным в DMZ, будут использоваться сети VACL. Это лишит злоумышленников возможности устанавливать несанкционированное исходящее соединение. Важно помнить, что серверы DMZ не только отображают трафик, соответствующий клиентским сеансам, но также используют такие дополнительные службы, как DNS (система доменных имен) и обнаружение пути MTU (максимальный блок передачи данных). Таким образом, ACL следует разрешить все службы, необходимые для серверов DMZ.

[Проверка транзитной DMZ](#)

На испытательном стенде мы реализовали сегмент DMZ с двумя маршрутизаторами, сконфигурированными как стеновые серверы: server_dmz1 и server_dmz2. Предполагается, что данные серверы доступны для внешних и внутренних клиентов, и аутентификация всех подключений HTTP выполняется с использованием внутреннего сервера RADIUS (CiscoSecure ACS для UNIX). Как внутренний, так и внешний маршрутизаторы настроены в качестве межсетевых экранов пакетной фильтрации. На рисунке ниже показана тестовая модель с используемой схемой адресации.

Рис. 3: Тестовая модель транзитной DMZ

Следующий список содержит основные шаги по настройке PVLAN. Маршрутизатор Catalyst 6500 используется как коммутатор L2 в DMZ.

- Server_dmz_1 подключен к порту 3/9
- Server_dmz_1 подключен к порту 3/10
- Внутренний маршрутизатор подключен к порту 3/34
- Внешний маршрутизатор подключен к порту 3/35

Были выбраны следующие виртуальные локальные сети:

- 41 – первичная сеть VLAN
- 42 – изолированная сеть VLAN

[Конфигурация частной сети VLAN](#)

Следующая конфигурация задает PVLANs на соответствующих портах.

```
ecomm-6500-2 (enable) set vlan 41 pvlan primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 41 configuration successful
```

```
ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type Ports
-----
```

```
41 - -
ecomm-6500-2 (enable) set vlan 42 pvlan isolated
VTP advertisements transmitting temporarily stopped,
```

```
and will resume after the command finishes.
Vlan 42 configuration successful
ecomm-6500-2 (enable) set pvlan 41 42 3/9-10
Successfully set the following ports to Private Vlan 41,42:
3/9-10
```

```
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/35
Successfully set mapping between 41 and 42 on 3/35
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/34
Successfully set mapping between 41 and 42 on 3/34
```

Port	Name	Status	Vlan	Duplex	Speed	Type
3/9	server_dmz1	connected	41,42	a-half	a-10	10/100BaseTX
3/10	server_dmz2	connected	41,42	a-half	a-10	10/100BaseTX
3/34	to_6500_1	connected	41	auto	auto	10/100BaseTX
3/35	external_router_dm	connected	41	a-half	a-10	10/100BaseTX

Конфигурация VACL в первичной VLAN

Данный раздел исключительно важен для повышения безопасности в зоне DMZ. [В разделе Известные ограничения VACL и PVLAN серверы, принадлежащие двум различным вторичным VLAN или таким же изолированным, предоставляют возможность злоумышленнику использовать их для взаимодействия друг с другом.](#) При попытке установить соединение между серверами на прямую, то сделать это на L2 не получится из-за PVLAN. Если злоумышленник несанкционированно проникает на серверы и настраивает их таким образом, что трафик для той же подсети отправляется маршрутизатору, трафик будет отправлен обратно в ту же подсеть и, таким образом, частная виртуальная локальная сеть перестанет выполнять свое назначение.

Поэтому список VACL нужно настраивать в первичной VLAN (VLAN передает трафик из маршрутизаторов) с использованием следующих политик:

- Разрешить трафик с IP-адресом маршрутизатора в качестве исходного IP-адреса
- Запретить трафик с IP-адресами источника и назначения, принадлежащими подсети DMZ

• Разрешите весь остальной трафик

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
```

```
-----
1. permit ip host 172.16.65.193 any
2. permit ip host 172.16.65.201 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

```
ecomm-6500-2 (enable) sh sec acl
ACL                               Type VLANs
-----
protect_pvlan                     IP      41
```

Список ACL не влияет на трафик, генерируемый серверами; он только предотвращает выполнение маршрутизаторами маршрутизации трафика, поступающего из серверов, обратно в ту же сеть VLAN. Первые два оператора позволяют маршрутизаторам отправлять сообщения, например icmp redirect или icmp unreachable, к серверам.

Конфигурация VACL на вторичной VLAN

Следующие журналы конфигурации показывают, как настроен VACL для фильтрации

трафика, созданного серверами. Настройка VACL преследует такие цели, как:

- Разрешить команду ping с серверов (разрешить команду echo)
- Предотвращение распространения ответов с серверов (с помощью команды echo)
- Разрешить HTTP соединения, исходящие изнутри
- Разрешить проверку подлинности RADIUS (UDP-порт 1645) и учет трафика (UDP-порт 1646)
- Разрешить DNS-трафик (UDP-порт 53)

Нужно запретить весь остальной трафик.

Что касается фрагментации, мы предполагаем следующее на сегменте сервера:

- Серверы не генерируют фрагментированный трафик
- Серверы могут получать фрагментированный трафик

При наличии оборудования PFC управляющего модуля 1 Catalyst 6500 лучше явно запретить фрагменты icmp. Причина заключается в том, что аппаратное обеспечение считает фрагменты ICMP и эхо-ответ одинаковыми, и по умолчанию оборудование запрограммировано на явное разрешение фрагментов. **Поэтому, если необходимо остановить пакеты эхо-ответа от сервера, необходимо в явном виде указать это с помощью команды deny icmp any any fragment.**

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out deny icmp any any fragment
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.199 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.202 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.199 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.202 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199 any eq 53
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202 any eq 53
```

```
ecomm-6500-2 (enable) Commit sec acl all
```

```
ecomm-6500-2 (enable) Set sec acl map dmz_servers_out 42
```

```
ecomm-6500-2 (enable) sh sec acl
```

ACL	Type	VLANs
protect_pvlan	IP	41
dmz_servers_out	IP	42

```
ecomm-6500-2 (enable) sh sec acl info dmz_servers_out
set security acl ip dmz_servers_out
```

```
-----
1. deny icmp any any fragment
2. permit icmp host 172.16.65.199 any echo
3. permit icmp host 172.16.65.202 any echo
4. permit tcp host 172.16.65.199 eq 80 any established
5. permit tcp host 172.16.65.202 eq 80 any established
6. permit udp host 172.16.65.199 eq 1645 host 172.16.171.9 eq 1645
```

7. permit udp host 172.16.65.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 172.16.65.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 172.16.65.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 172.16.65.199 any eq 53
11. permit udp host 172.16.65.202 any eq 53

Тестирование конфигурации

Были получены следующие выходные данные, когда настроены сети PVLAN, а списки VACL не применены. Проверка показывает, что из внешнего маршрутизатора пользователь может осуществить команду ping к внутреннему маршрутизатору, также как и к серверам.

```
external_router#ping 172.16.65.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!
```

```
external_router#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
external_router#ping 172.16.65.199
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

В следующем примере показано, что можно осуществить команду ping с серверов на внешние сети, шлюз по умолчанию, но не на серверы, принадлежащие к той же вторичной VLAN.

```
server_dmz1#ping 203.5.6.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.5.6.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

```
server_dmz1#ping 172.16.65.202
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

После составления списков VACL команда ping из внешнего маршрутизатора больше не проходит:

```
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

На следующем примере можно увидеть сервер, получающий запросы HTTP GET из внутренней сети:

```
server_dmz1#debug ip http url
```

```
HTTP URL debugging is on
server_dmz1#debug ip http tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar 7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar 7 09:24:03.092 PST: HTTP: client version 1.0
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar 7 09:24:03.092 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:03.092 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar 7 09:24:03.092 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar 7 09:24:03.092 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:03.092 PST: HTTP: parsed line gzip
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:03.096 PST: HTTP: parsed line en
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:03.096 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar 7 09:24:03.096 PST: HTTP: authorization rejected
*Mar 7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar 7 09:24:22.532 PST: HTTP: client version 1.0
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar 7 09:24:22.532 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:22.532 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar 7 09:24:22.532 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar 7 09:24:22.532 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:22.532 PST: HTTP: parsed line gzip
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:22.532 PST: HTTP: parsed line en
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:22.532 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar 7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar 7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar 7 09:24:22.904 PST: HTTP: received GET ''
```

Внешняя безопасная зона

Внешний сценарий DMZ является, возможно, наиболее приемлемой и широко используемой реализацией. Внешняя демилитаризованная зона (DMZ) реализуется с помощью одного или нескольких интерфейсов межсетевого экрана, как показано на рисунке ниже.

Рис. 4: Внешняя безопасная зона

Обычно требования для DMZ стремятся к однообразию, независимо от реализации проекта. Как и в предыдущем случае, серверы DMZ доступны как из внешних клиентов, так и из внутренней сети. В итоге серверам DMZ будет необходим доступ к некоторым внутренним ресурсам, а их взаимодействие не предполагается. При этом трафик не должен

иницироваться из DMZ в Internet; такие серверы DMZ только выводят ответный трафик, соответствующий внешним соединениям.

Так же как и в предыдущем случае, первый шаг конфигурации заключается в достижении изоляции на уровне L2 с помощью сетей PVLAN, так что серверы DMZ не взаимодействуют друг с другом, тогда как внутренние и внешние хосты имеют к ним доступ. Это достигается за счет настройки серверов в дополнительной сети VLAN с изолированными портами. Межсетевой экран определяется в первичной VLAN со смешанным портом. Брандмауэр будет единственным устройством внутри этой основной VLAN.

Вторым шагом является определение списков ACL для управления трафиком, иницируемым в DMZ. При определении списков ACL следует разрешить только необходимый трафик.

[Проверка внешней DMZ](#)

На следующем рисунке показан тестовый стенд, собранный для Примера практического применения, в котором мы использовали межсетевой экран PIX с третьим интерфейсом для DMZ. Такой же набор маршрутизаторов используется в качестве веб-серверов, а все сеансы HTTP аутентифицируются одним и тем же сервером RADIUS.

Рис. 5: Тестовая модель внешней DMZ

В этот сценарий мы включили только наиболее интересную выборку файлов конфигурации, так как конфигурации PVLAN и VACL были подробно объяснены в предыдущем практическом примере.

[Конфигурация PIX](#)

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip http tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line 172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
```

```
*Mar 7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar 7 09:24:22.532 PST: HTTP: client version 1.0
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar 7 09:24:22.532 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:22.532 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar 7 09:24:22.532 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar 7 09:24:22.532 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:22.532 PST: HTTP: parsed line gzip
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:22.532 PST: HTTP: parsed line en
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:22.532 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar 7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar 7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar 7 09:24:22.904 PST: HTTP: received GET ''
```

[Конфигурация RADIUS](#)

Конфигурация NAS

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip http tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar 7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar 7 09:24:03.092 PST: HTTP: client version 1.0
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar 7 09:24:03.092 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:03.092 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar 7 09:24:03.092 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar 7 09:24:03.092 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:03.092 PST: HTTP: parsed line gzip
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:03.096 PST: HTTP: parsed line en
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:03.096 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar 7 09:24:03.096 PST: HTTP: authorization rejected
*Mar 7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar 7 09:24:22.532 PST: HTTP: client version 1.0
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar 7 09:24:22.532 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:22.532 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar 7 09:24:22.532 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept
```

```
*Mar 7 09:24:22.532 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:22.532 PST: HTTP: parsed line gzip
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:22.532 PST: HTTP: parsed line en
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:22.532 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar 7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar 7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar 7 09:24:22.904 PST: HTTP: received GET ''
```

Сервер RADIUS CSUX

```
server_dmz1#debug ip http url
```

```
HTTP URL debugging is on
```

```
server_dmz1#debug ip http tran
```

```
HTTP transactions debugging is on
```

```
server_dmz1#debug ip http auth
```

```
HTTP Authentication debugging is on
```

```
server_dmz1#
```

```
*Mar 7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar 7 09:24:03.092 PST: HTTP: client version 1.0
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar 7 09:24:03.092 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:03.092 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar 7 09:24:03.092 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar 7 09:24:03.092 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:03.092 PST: HTTP: parsed line gzip
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:03.096 PST: HTTP: parsed line en
*Mar 7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:03.096 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
```

```
*Mar 7 09:24:03.096 PST: HTTP: authorization rejected
*Mar 7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar 7 09:24:22.532 PST: HTTP: client version 1.0
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar 7 09:24:22.532 PST: HTTP: parsed line Keep-Alive
*Mar 7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar 7 09:24:22.532 PST: HTTP: parsed line Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar 7 09:24:22.532 PST: HTTP: parsed line 172.16.65.199
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar 7 09:24:22.532 PST: HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar 7 09:24:22.532 PST: HTTP: parsed line gzip
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar 7 09:24:22.532 PST: HTTP: parsed line en
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar 7 09:24:22.532 PST: HTTP: parsed line iso-8859-1,*,utf-8
*Mar 7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar 7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar 7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15 privless '/'
*Mar 7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
```


Настройка Catalyst

Нужно обратить внимание, что в этой конфигурации нет необходимости в настройке конфигурации VACL в основной виртуальной локальной сети, так как PIX не перенаправляет трафик к интерфейсу, от которого они получен. [VACL, описанный в конфигурации VACL в разделе "Первичная VLAN", должен быть избыточным.](#)

```
set security acl ip dmz_servers_out
-----
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
6. permit udp host 199.5.6.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 199.5.6.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 199.5.6.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 199.5.6.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 199.5.6.199 any eq 53
11. permit udp host 199.5.6.202 any eq 53
ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type Ports
-----
41      42      isolated      3/9-10

ecomm-6500-2 (enable) sh pvlan mapping
Port Primary Secondary
-----
3/14 41      42
3/34 41      42
3/35 41      42
ecomm-6500-2 (enable) sh port
Port Name Status Vlan Duplex Speed Type
-----
3/9 server_dmz1 connected 41,42 a-half a-10 10/100BaseTX
3/10 server_dmz2 connected 41,42 a-half a-10 10/100BaseTX
3/14 to_pix_port_2 connected 41 full 100 10/100BaseTX
3/35 external_router_dm notconnect 41 auto auto 10/100BaseTX
```

Концентратор VPN параллельно с межсетевым экраном

При реализации доступа к виртуальным частным сетям (VPN), одним из предпочтительных методов является, несомненно, параллельная структура (см. рисунок ниже). Заказчики обычно предпочитают данный метод, так как он прост в применении, почти не влияет на существующую инфраструктуру и легко масштабируется на основе гибкости устройств.

В параллельном методе концентратор VPN подключается к внутреннему и внешнему сегментам. Все сеансы VPN завершаются в концентраторе, не проходя через межсетевой экран. Обычно предполагается, что клиентам VPN предоставляется неограниченный доступ к внутренней сети, однако иногда права доступа клиентов могут быть ограничены несколькими серверами (группой серверов с одним IP-адресом). Одной из оптимальных функций является разделение трафика VPN и регулярного Интернет-трафика. Так, например, клиентам VPN не разрешен доступ в Интернет через корпоративный межсетевой экран.

Рис. 6: Концентратор VPN параллельно с межсетевым экраном

[Проверка концентратора VPN параллельно с межсетевым экраном](#)

В данном примере используется концентратор VPN 5000, установленный вместе с межсетевым экраном PIX. Два маршрутизатора, настроенные в качестве веб-серверов, установлены во внутреннем сегменте как внутренняя ферма серверов. Клиентам виртуальной частной сети разрешен только доступ к группе серверов, а трафик Internet должен быть отделен от трафика виртуальной локальной сети (IPSec). На рисунке ниже показана тестовая модель.

Рисунок 7: Тестовая модель концентратора VPN параллельно с межсетевым экраном

В этом сценарии присутствуют две главные области, представляющие интерес:

- Внутренний коммутатор L2
- Внешний маршрутизатор L2

Потоки трафика для внутреннего коммутатора L2 определяются на основе следующих инструкций:

- Клиенты VPN имеют полный доступ к заданному набору внутренних серверов (ферме серверов)
- Внутренним клиентам также разрешен доступ на серверную ферму
- Внутренние клиенты имеют неограниченный доступ в Интернет
- Трафик, приходящий от концентратора VPN, нужно изолировать от межсетевого экрана PIX

Потоки трафика для внешнего коммутатора L2 определены, как показано ниже:

- Трафик, полученный от маршрутизатора, должен иметь возможность дойти до VPN-концентратора или PIX
- Трафик, исходящий из PIX, необходимо изолировать от трафика, исходящего из VPN

Возможно, администратор пытается предотвратить поступление трафика из внутренней сети на узлы VPN; это можно выполнить, настроив VACL в основной сети VLAN (VACL будет отфильтровывать только трафик, исходящий от внутреннего маршрутизатора; на остальной трафик это не повлияет).

[Конфигурация PVLAN](#)

Так как главной задачей в структуре является сохранение трафика, исходящего из PIX и отделенного от трафика сервера и концентратора VPN, необходимо настроить PIX на сети PVLAN, отличной от PVLAN, на которой настраиваются серверы и концентратор VPN.

Трафик, исходящий из внутренней сети, должен иметь доступ к ферме серверов, а также к VPN-концентратору и PIX. В результате порт, подключающийся ко внутренней сети, будет смешанным портом.

Серверы и VPN-концентратор принадлежат одной вторичной VLAN и могут взаимодействовать.

Что касается внешнего коммутатора L2, маршрутизатор, предоставляющий доступ к Интернету (принадлежащий обычно поставщику Интернет-услуг (ISP)), соединен со смешанным портом, в то время как VPN-концентратор и PIX принадлежат одним и тем же

частным и изолированным VLAN (поэтому они не могут обмениваться трафиком). Таким образом, трафик, поступающий от поставщика услуг, может выбрать либо путь к концентратору VPN, либо путь к PIX. PIX и концентратор VPN обладают большей степенью защищенности по причине их изолированности.

Конфигурация PVLAN для внутреннего коммутатора L2

```
sh pvlan
```

```
Primary Secondary Secondary-Type Ports
-----
41      42      community      3/7,3/9-10
41      43      isolated       3/12
```

```
ecommm-6500-2 (enable) sh pvlan map
```

```
Port Primary Secondary
```

```
-----
```

```
3/34 41      42-43
```

```
ecommm-6500-2 (enable) sh port 3/7
```

```
Port Name Status Vlan Duplex Speed Type
-----
3/7 to_vpn_conc connected 41,42 a-half a-10 10/100BaseTX
```

```
ecommm-6500-2 (enable) sh port 3/9
```

```
Port Name Status Vlan Duplex Speed Type
-----
3/9 server_1 connected 41,42 a-half a-10 10/100BaseTX
```

```
ecommm-6500-2 (enable) sh port 3/10
```

```
Port Name Status Vlan Duplex Speed Type
-----
3/10 server_2 connected 41,42 a-half a-10 10/100BaseTX
```

```
ecommm-6500-2 (enable) sh port 3/12
```

```
Port Name Status Vlan Duplex Speed Type
-----
3/12 to_pix_intf1 connected 41,43 a-full a-100 10/100BaseTX
```

```
ecommm-6500-2 (enable) sh pvlan map
```

```
Port Primary Secondary
```

```
-----
```

```
3/34 41      42-43
```

```
ecommm-6500-2 (enable) sh port 3/34
```

```
Port Name Status Vlan Duplex Speed Type
-----
3/34 to_int_router connected 41 a-full a-100 10/100BaseTX
```

Конфигурация PVLAN внешнего коммутатора L2

```
sh pvlan
```

```
Primary Secondary Secondary-Type Ports
-----
41      45      isolated       3/7,3/33
```

```
ecommm-6500-1 (enable) sh pvlan mapping
```

```
Port Primary Secondary
```

```
-----
```

```

ecomm-6500-1 (enable) sh port 3/7
Port Name                Status      Vlan      Duplex Speed Type
-----
3/7  from_vpn              connected  41,45     a-half  a-10  10/100BaseTX

```

```

ecomm-6500-1 (enable) sh port 3/33
Port Name                Status      Vlan      Duplex Speed Type
-----
3/33 to_pix_intf0         connected  41,45     a-full  a-100 10/100BaseTX

```

```

ecomm-6500-1 (enable) sh pvlan map
Port Primary Secondary
-----
3/43 41      45

```

```

ecomm-6500-1 (enable) sh port 3/43
Port Name                Status      Vlan      Duplex Speed Type
-----
3/43 to_external_router connected  41         a-half  a-10  10/100BaseTX

```

Тестирование конфигурации

Этот эксперимент показывает, что внутренний маршрутизатор проходит через межсетевой экран и достигает внешнего маршрутизатора (маршрутизатор внешнего межсетевого экрана с интерфейсом 198.5.6.1).

ping 198.5.6.1

```

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```

Этот эксперимент показывает следующее (все данные из сервера 1):

- Сервер 1 может выполнить эхо-тест внутреннего маршрутизатора: **server_1#ping 172.16.65.193**

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

- Сервер 1 может выполнить эхо-запрос VPN-концентратора: **server_1#ping 172.16.65.203**

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.203, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

- Серверу Server 1 не удалось проверить доступность внутреннего интерфейса PIX: **server_1#ping 172.16.65.201**

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.201, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

- Сервер 1 не может выполнить эхо-тест внешнего маршрутизатора: **server_1#ping 198.5.6.1**

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....

```

Success rate is 0 percent (0/5)

В следующем эксперименте показано, что сеансы HTTP можно открывать из внутренней сети для фермы серверов.

```
server_1#ping 198.5.6.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

В следующем эксперименте показано, что трафик HTTP из сети VPN идет к ферме серверов (обратите внимание на IP-адрес 10.1.1.1).

```
server_1#ping 198.5.6.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Ниже приведена конфигурация концентратора VPN:

```
server_1#ping 198.5.6.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Следующая команда отображает список подключенных пользователей:

```
sh VPN user
```

Port	User	Group	Client Address	Local Address	ConnectNumber Time
VPN 0:1	martin	RemoteUsers	206.1.1.10	10.1.1.1	00:00:11:40

Следует отметить, что шлюз по умолчанию на серверах является внутренним маршрутизатором 172.16.65.193, который выдает команду `ip redirect` к маршрутизатору 172.16.65.203. Эта реализация вызывает неоптимальные потоки трафика, потому что хост посылает первый пакет потока маршрутизатору и при получении переадресованного он отошлет последующие пакеты шлюзу, более подходящему для обработки этого трафика. Другой способ: можно настроить два различных маршрута непосредственно на серверах, чтобы указать VPN-концентратор для IP-адресов 10.x.x.x и маршрутизатор 172.16.65.193 для остального трафика. Если на серверах настроен шлюз по умолчанию, необходимо убедиться, что для интерфейса маршрутизатора настроен "ip redirect".

Любопытная особенность, которую мы заметили при тестировании, состоит в следующем. При попытке отослать команду `ping` на внешний IP-адрес 198.5.6.1 из серверов или VPN, шлюз по умолчанию отошлет команду `ip redirect` на 172.16.65.201.

```
sh VPN user
```

Port	User	Group	Client Address	Local Address	ConnectNumber Time
VPN 0:1	martin	RemoteUsers	206.1.1.10	10.1.1.1	00:00:11:40

На этом этапе серверы или VPN-концентратор отправляют запрос ARP (протокол разрешения адреса) для 172.16.65.201 и не получают ответ от 201, так как это другая вторичная VLAN; вот что предлагает нам сеть PVLAN. В реальности это простой способ

обойти проблему, то есть послать трафик к MAC .193 или с назначением IP 172.16.65.201.

Маршрутизатор .193 направит трафик обратно на тот же интерфейс, но, поскольку интерфейсом маршрутизатора является случайный порт, трафик поступит на .201, что нежелательно. [Эта проблема была рассмотрена в разделе "Известные ограничения VACL и PVLAN"](#).

[Конфигурация VACL](#)

Данный раздел исключительно важен для повышения безопасности на ферме серверов. [Как описано в разделе Известные ограничения VACL и PVLAN, даже если серверы и межсетевой экран PIX принадлежат двум различным вторичным VLAN, злоумышленник все же имеет способ заставить их взаимодействовать друг с другом.](#) Если они попытаются связаться напрямую, они не смогут это сделать из-за сетей PVLAN. Если злоумышленник несанкционированно проникает на серверы и настраивает их таким образом, что трафик для той же подсети отправляется маршрутизатору, трафик будет отправлен обратно в ту же подсеть и, таким образом, частная виртуальная локальная сеть перестанет выполнять свое назначение.

Поэтому список VACL нужно настраивать в первичной VLAN (VLAN передает трафик из маршрутизаторов) с использованием следующих политик:

- Разрешить трафик с IP-адресом маршрутизатора в качестве исходного IP-адреса
- Запретите трафик с IP-адресами источника и назначения, принадлежащими подсети фермы серверов
- Разрешите весь остальной трафик

```
ecommm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
-----
1. permit ip host 172.16.65.193 any
2. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
3. permit ip any any
```

```
ecommm-6500-2 (enable) sh sec acl
ACL                               Type  VLANS
-----
protect_pvlan                     IP    41
```

Список ACL не влияет на трафик, генерируемый серверами или PIX; он только предотвращает выполнение маршрутизаторами маршрутизации трафика, поступающего из серверов, обратно в ту же сеть VLAN. Первые два оператора позволяют маршрутизаторам отправлять сообщения, например icmp redirect или icmp unreachable, к серверам.

Обнаружен еще один трафик, который может быть остановлен администратором с помощью VACL. Этот поток направляется из внутренней сети к узлам VPN. Для того, чтобы его остановить, VACL сопоставляется с первичной VLAN (41) и объединяется с предыдущим:

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
```


3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any

Тестирование конфигурации

Отправка эхо-запроса хоста 10.1.1.1 из маршрутизатора .193 (zundapp). До сопоставления с VACL команда ping проходит успешно.

```
show sec acl info all
```

```
set security acl ip protect_pvlan
```

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any

После сопоставления с VACL на VLAN 41 та же самая команда ping не будет успешной:

```
show sec acl info all
```

```
set security acl ip protect_pvlan
```

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any

Однако это не мешает отправить команду ping внешнему маршрутизатору:

```
show sec acl info all
```

```
set security acl ip protect_pvlan
```

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any

Дополнительные сведения

- [Настройка списков управления доступом – документация по Catalyst 6000](#)
- [Техническая поддержка - Cisco Systems](#)