Программно-аппаратный комплекс ViPNet IDS 2.4

Руководство по установке и обновлению ViPNet IDS VA

infotecs

ФРКЕ.00120-06 90 04

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1

Тел: (495) 737-61-96 (горячая линия), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Для кого предназначен документ

Данный документ предназначен для администраторов, отвечающих за эксплуатацию и сопровождение ViPNet IDS.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

1

Общие сведения

Назначение ПАК ViPNet IDS

Программно-аппаратный комплекс ViPNet IDS (далее — ViPNet IDS) является интегрированным решением на базе специализированной аппаратной платформы и программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС Linux. Программно-аппаратный комплекс ViPNet IDS является средством обнаружения компьютерных атак и используется в сетях для повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

Обнаружение сетевых атак происходит на основе анализа сетевого трафика, начиная с канального и заканчивая прикладным уровнем модели взаимодействия открытых систем (OSI). Анализ данных с целью обнаружения атак осуществляется с использованием сигнатурного и эвристического методов, а также производится анализ трафика препроцессорами, встроенными в ViPNet IDS.

При обнаружении компьютерной атаки ViPNet IDS идентифицирует событие, регистрирует факт обнаружения атаки и оповещает администратора о данном событии. Оповещение может производиться с помощью следующих способов:

- веб-интерфейса ViPNet IDS;
- передачи параметров в ПК ViPNet StateWatcher по протоколу SNMP;
- передачи параметров в различные системы управления событиями информационной безопасности (SIEM, ESM и так далее) по протоколам syslog, syslog (в формате CEF) или SNMP;
- уведомления по электронной почте.

Эта информация позволяет администратору своевременно предотвратить атаку с помощью средств сетевого экранирования, а также может быть использована для анализа защищенности сети и разработки комплекса мер по недопущению подобных инцидентов в будущем.

Требования к виртуальной среде ViPNet IDS VA

ViPNet IDS имеет программный вариант исполнения ViPNet IDS VA, который предназначен для развертывания на платформе виртуализации. Поддерживается работа ViPNet IDS VA на следующих платформах виртуализации:

- VMware ESXi версии 5;
- VMware Workstation версий 8 — 11;
- Oracle VM VirtualBox версий 4.3.34 — 5.0.10.

Внимание! В связи с тем, что ViPNet IDS VA поставляется в формате стандарта OVF (Open Virtualization Format), он может быть установлен на любой современной платформе виртуализации. Однако работоспособность в этом случае не гарантируется.

2

Подготовка ViPNet IDS VA к работе

Порядок действий

Для подготовки ViPNet IDS VA к работе выполните все действия из приведенного ниже списка.

Примечание. Описание развертывания ViPNet IDS VA приведено на примере платформы виртуализации VMware ESXi. Предполагается, что в сети уже развернут сервер ESXi (vCenter Server) и настроено подключение к нему клиентов VMware vSphere Client.

Таблица 3. Последовательность действий по подготовке ViPNet IDS VA к работе

	Действие	Ссылка
☐	Произведите анализ сети, в которую планируется подключить ViPNet IDS	Анализ сети, в которую планируется внедрение ViPNet IDS (на стр. 12)
☐	Определите способ подключения ViPNet IDS в вашу сеть	Способы подключения ViPNet IDS в сети вашей организации (на стр. 13)
☐	Установите виртуальный образ ViPNet IDS VA на платформу виртуализации	Установка ViPNet IDS VA на платформу виртуализации (на стр. 17)
☐	В зависимости от способа организации вашей сети и ваших потребностей по выявлению аномалий сетевого трафика сконфигурируйте сетевой интерфейс, который будет работать на ViPNet IDS как интерфейс захвата трафика	Конфигурирование интерфейсов захвата трафика (на стр. 19)
☐	Запустите ViPNet IDS VA. При первом запуске смените пароль администратора системы, заданный по умолчанию	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Первый запуск ViPNet IDS. Смена пароля администратора системы»
☐	Произведите настройку управляющего интерфейса в IDS Консольном конфигураторе	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Изменение настроек управляющего интерфейса ViPNet IDS»
☐	Задайте часовой пояс и системное время на ViPNet IDS в IDS Консольном конфигураторе	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Задание системного времени и часового пояса на ViPNet IDS»

	Действие	Ссылка
☐	Подключитесь к веб-интерфейсу ViPNet IDS для дальнейших настроек ViPNet IDS и смените пароль по умолчанию для главного администратора	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Подключение к веб-интерфейсу ViPNet IDS и завершение работы с ним» и раздел «Смена пароля главного администратора при первом подключении к веб-интерфейсу»
☐	Создайте файл с запросом на лицензию ViPNet IDS и отправьте его в отдел технического сопровождения ОАО «ИнфоТеКС», отвечающий за лицензирование	Создание запроса на лицензию (на стр. 30)
☐	После получения лицензии установите ее на ViPNet IDS	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Установка лицензии на ViPNet IDS»
☐	Загрузите с Сервера обновлений «ОАО ИнфоТеКС» и установите на ViPNet IDS последнюю версию базы правил обнаружения атак	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Первоначальная установка правил обнаружения атак»
☐	Произведите настройки параметров обработки трафика защищаемой сети	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Настройка параметров обработки трафика защищаемой сети»
☐	Создайте SnapShot виртуальной машины, который может потребоваться вам для восстановления виртуальной машины в случае сбоя.	В соответствии с документацией к используемой виртуальной среде

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Анализ сети, в которую планируется внедрение ViPNet IDS

Перед вводом ViPNet IDS в эксплуатацию необходимо проанализировать вашу сеть с целью выявления ее конфигурации и всех объектов, которые необходимо защитить от возможных атак. В результате анализа сети вы должны иметь следующую информацию:

- структуру защищаемой сети;
- сетевые сервисы, которые функционируют в сети;
- используются ли в сети проприетарные протоколы передачи данных;
- используемые в сети серверы, атака на которые может быть наиболее критична для компании;
- сервисы, доступные из внешней сети (из Интернета).

Эти данные необходимы для дальнейшей настройки ViPNet IDS.

Анализ сети и последующую конфигурацию ViPNet IDS под конкретную сеть должен производить аналитик по информационной безопасности, имеющий глубокие знания в сфере сетевых технологий и опыт в расследовании инцидентов безопасности.

Способы подключения ViPNet IDS в сети вашей организации

ViPNet IDS может быть установлен в сети одним из следующих способов:

1. после межсетевого экрана (то есть со стороны защищаемой сети). Этот способ является оптимальным в случае высоких нагрузок на сеть;
2. до межсетевого экрана (то есть со стороны открытой сети);
3. до и после межсетевого экрана.

Также для развертывания ViPNet IDS в сети необходим коммутатор со SPAN-портом (см. глоссарий, стр. 35) или ответвитель трафика TAP (на стр. 36), который будет улавливать весь сетевой трафик и зеркалировать его на интерфейс захвата трафика ViPNet IDS (см. глоссарий, стр. 36). Использование SPAN-порта коммутатора или ответвителя трафика TAP позволяет получить копию внешнего сетевого трафика, не мешая при этом функционированию сети.

Внимание! Коммутатор со SPAN-портом и ответвитель трафика TAP не входят в комплект поставки.

Рассмотрим подробнее эти три способа подключения.

1. Подключение ViPNet IDS после межсетевого экрана. Чаще всего системы обнаружения атак устанавливают после межсетевого экрана, чтобы анализировать только те атаки, которые не были отражены межсетевым экраном.

   Схема подключения ViPNet IDS после межсетевого экрана представлена ниже.

Рисунок 1. Подключение ViPNet IDS после межсетевого экрана

   При таком способе включения:

   - нагрузка на ViPNet IDS снижается (часть трафика отсекается межсетевым экраном);

- объем информации, поступающей администратору ViPNet IDS, уменьшается;
- появляется возможность настройки правил на межсетевом экране с целью блокировки выявленных атак.

Кроме того, такой способ включения позволяет выявлять атаки внутри защищенного контура не только от внешних нарушителей, пропущенные межсетевым экраном, но и атаки со стороны внутренних нарушителей (при соответствующих настройках сети).

2 Подключение ViPNet IDS до межсетевого экрана. Также вы можете установить ViPNet IDS до межсетевого экрана, это позволит получать наиболее полную информацию об атаках со стороны внешних нарушителей, как прошедших в защищаемый контур через межсетевой экран, так и о несостоявшихся попытках сетевых атак, заблокированных межсетевым экраном.

Схема подключения ViPNet IDS до межсетевого экрана представлена ниже.

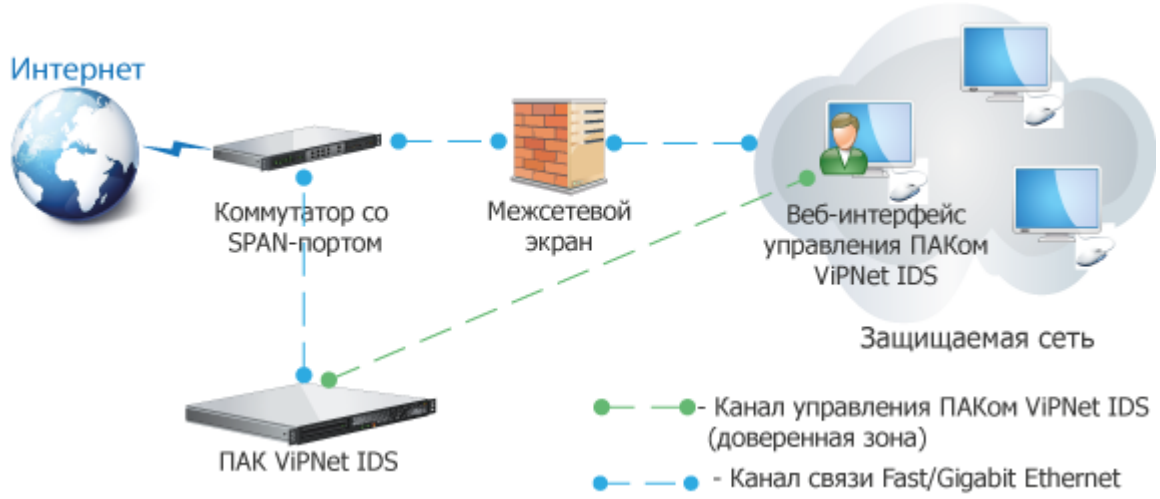

Рисунок 2. Подключение ViPNet IDS до межсетевого экрана

Однако при этом:

- возрастает нагрузка на ViPNet IDS;
- исключается возможность анализа трафика внутри защищенного контура;
- исключается возможность анализа эффективности работы правил блокировки атак, настроенных на межсетевом экране.

3 Подключение ViPNet IDS до и после сетевого экрана. Этот способ подключения является оптимальным, поскольку объединяет полезные возможности двух предыдущих способов и позволяет выявлять все попытки атак на сеть, как удачные, так и неудачные.

Схема подключения ViPNet IDS до и после межсетевого экрана представлена ниже.

Рисунок 3. Подключение ViPNet IDS до и после межсетевого экрана

3

Развертывание виртуального образа ViPNet IDS VA

Установка ViPNet IDS VA на платформу виртуализации

Для установки ViPNet IDS VA на платформу виртуализации вам потребуется файл с образом виртуальной машины в формате OVA, входящий в комплект поставки.

Чтобы установить ViPNet IDS VA, выполните следующие действия:

1. Запустите программу VMware vSphere Client и подключитесь к серверу vCenter Server.
2. В главном окне **vSphere Client** в меню **File** выберите пункт **Delploy OVF Template.**
3. В появившемся окне мастера **Deploy OVF Template** выберите файл `*.ova` с образом виртуальной машины и нажмите кнопку **Next**.

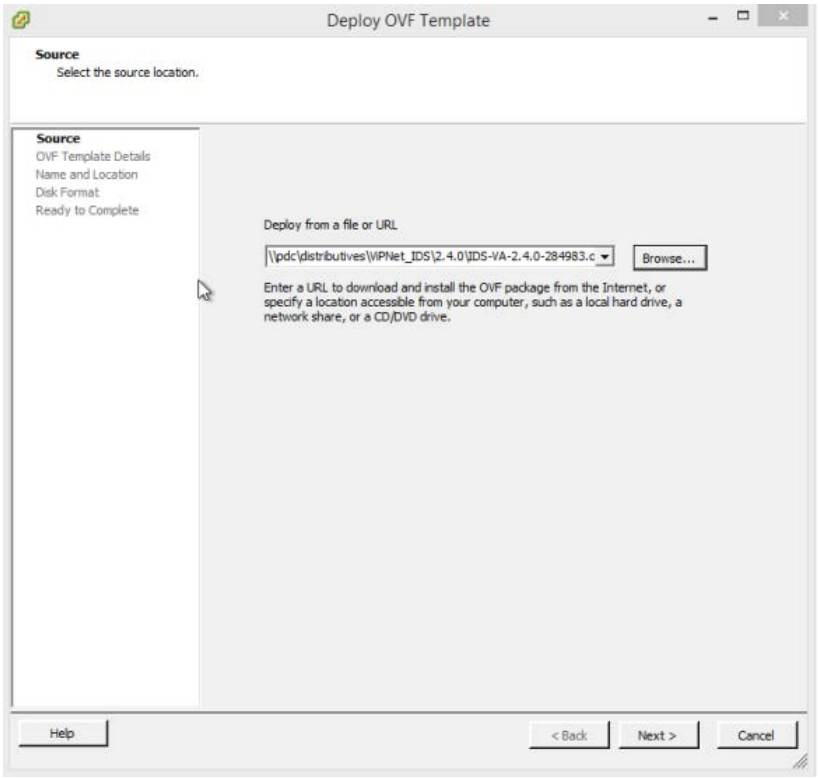

Рисунок 4. Выбор файла с образом виртуальной машины

4. На странице **OVF Template Details** с деталями устанавливаемого образа нажмите кнопку **Next**.
5. На странице **Name and Location** введите имя виртуальной машины и нажмите кнопку **Next**.
6. На странице **Disk Format** выберите тип диска **Thin Provision**, установив переключатель в одноименное положение, и нажмите кнопку **Next**.

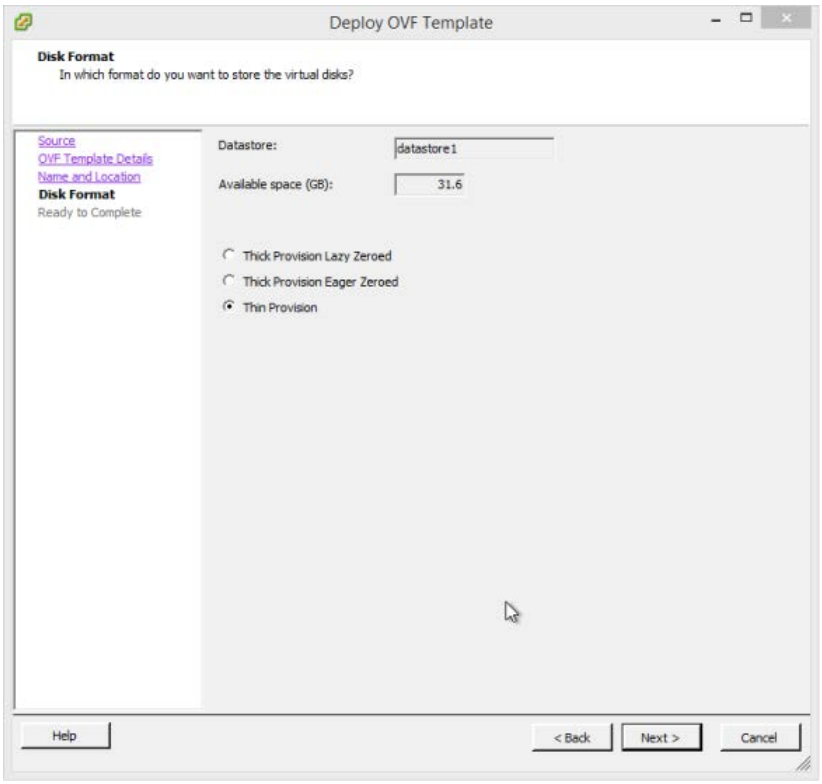

Рисунок 5. Выбор типа диска

7 На странице **Ready to Complete** нажмите кнопку **Finish**.

8 Дождитесь завершения процесса создания виртуальной машины.

В результате будет создана виртуальная машина с заданным вами именем, на которой установлено ПО ViPNet IDS VA.

Далее произведите конфигурирование сетевого интерфейса для захвата трафика (см. «Конфигурирование интерфейсов захвата трафика» на стр. 19).

Конфигурирование интерфейсов захвата трафика

ViPNet IDS VA позволяет анализировать сетевой трафик, поступающий как из физических локальных сетей, так и из виртуальных локальных сетей, организованных с помощью виртуальных сетевых коммутаторов.

В зависимости от способа организации вашей сети и ваших потребностей по выявлению аномалий сетевого трафика, необходимо произвести настройки интерфейсов захвата трафика ViPNet IDS, на которые будет передаваться весь трафик локальных сетей для его дальнейшего анализа на предмет наличия атак.

В данном документе рассмотрим варианты настроек интерфейсов захвата трафика для организации анализа сетевого трафика следующих типов локальных сетей:

- Настройки подключения для организации анализа трафика физической локальной сети (на стр. 19).
- Настройки подключения для организации анализа трафика виртуальной локальной сети (на стр. 25).
- Настройки подключения комбинированного варианта (на стр. 29).

Внимание! ViPNet IDS VA поддерживает работу до 4 сетевых интерфейсов, один из которых должен быть выделен под управляющий интерфейс, а остальные могут быть назначены интерфейсами захвата трафика.

Настройки подключения для организации анализа трафика физической локальной сети

Схема подключения ViPNet IDS VA для анализа сетевого трафика физической локальной сети представлена ниже.

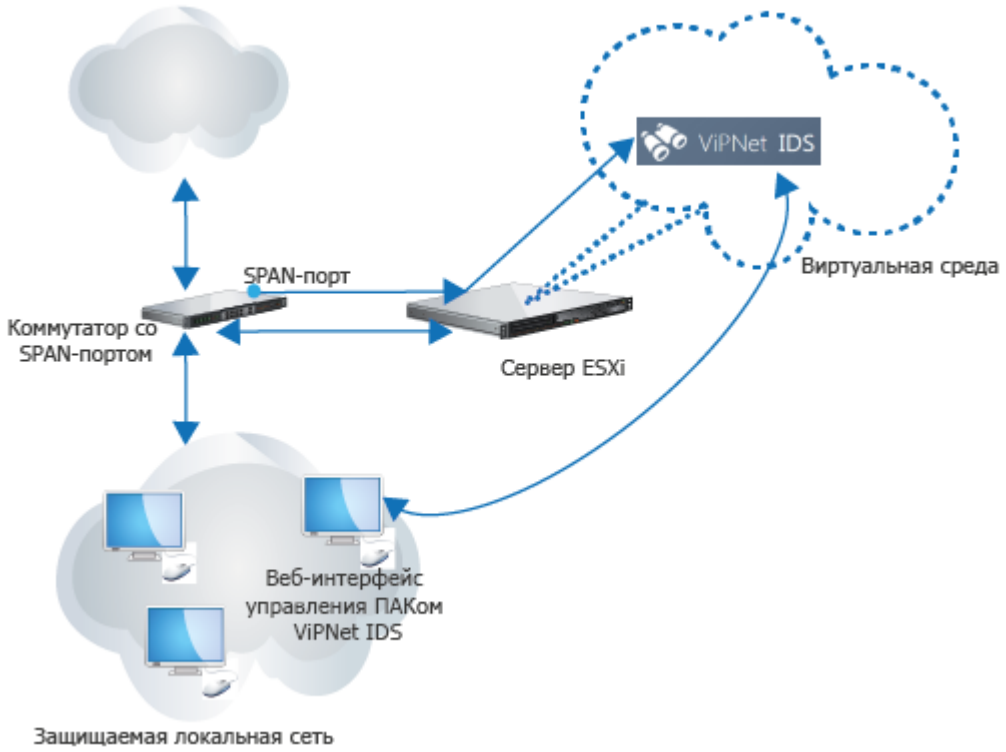

Рисунок 6. Схема подключения ViPNet IDS VA для анализа сетевого трафика физической локальной сети

Для настройки сетевого интерфейса, который будет использоваться как интерфейс захвата трафика ViPNet IDS, необходимо выделить физический сетевой адаптер на сервере ESXi (vCenter Server), создать для него виртуальный коммутатор (standard switch) и произвести его настройки. Настройки должны обеспечить подключение интерфейса захвата трафика к SPAN-порту коммутатора, чтобы интерфейс захвата смог получать трафик физических локальных сетей, подключенных через этот коммутатор.

Для настройки интерфейса захвата выполните следующие действия:

1 В настройках сетевых адаптеров сервера ESXi выберите свободный сетевой адаптер, который будет использоваться для передачи сетевого трафика на интерфейс захвата трафика ViPNet IDS.

Примечание. Этот сетевой адаптер должен быть подключен к SPAN-порту коммутатора.

---

2 В настройках vSphere Client введите данный адаптер в действие. Для этого:

2.1 Запустите программу VMware vSphere Client и подключитесь к серверу ESXi (vCenter Server).

2.2 Откройте вкладку **Configuration** и слева на панели навигации **Hardware** выберите **Networking**.

2.3 В окне просмотра виртуальных коммутаторов щелкните **Add Networking**.

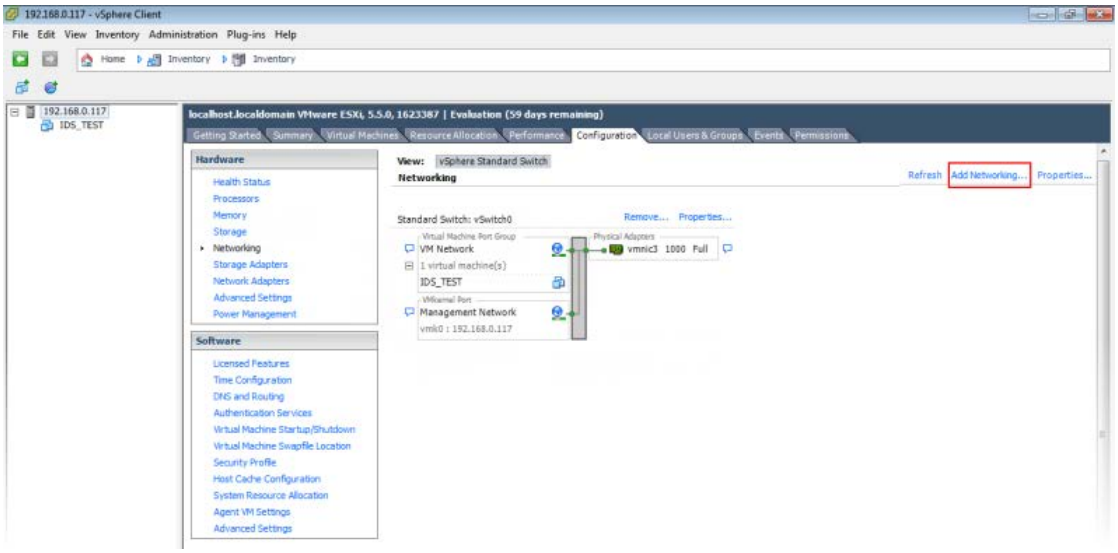

Рисунок 7. Свойства сетевого коммутатора

2.4 В появившемся окне мастера создания виртуальной сети **Add Network Wizard** выберите **Virtual Machine** и нажмите кнопку **Next**.

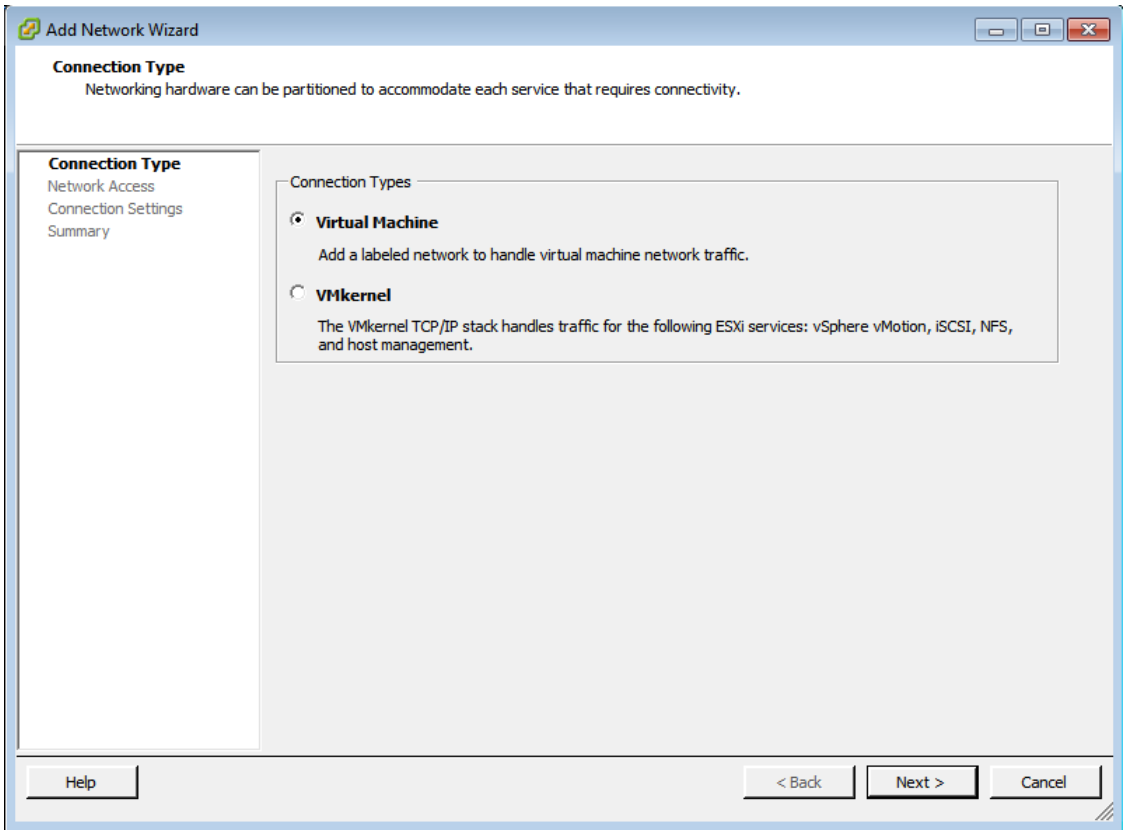

Рисунок 8. Добавление виртуальной сети

2.5 На странице **Network Acces** выберите **Create a vSphere standard switch** и установите флажок напротив сетевого адаптера, который вы выбрали в настройках сервера ESXi для передачи сетевого трафика на интерфейс захвата трафика ViPNet IDS.

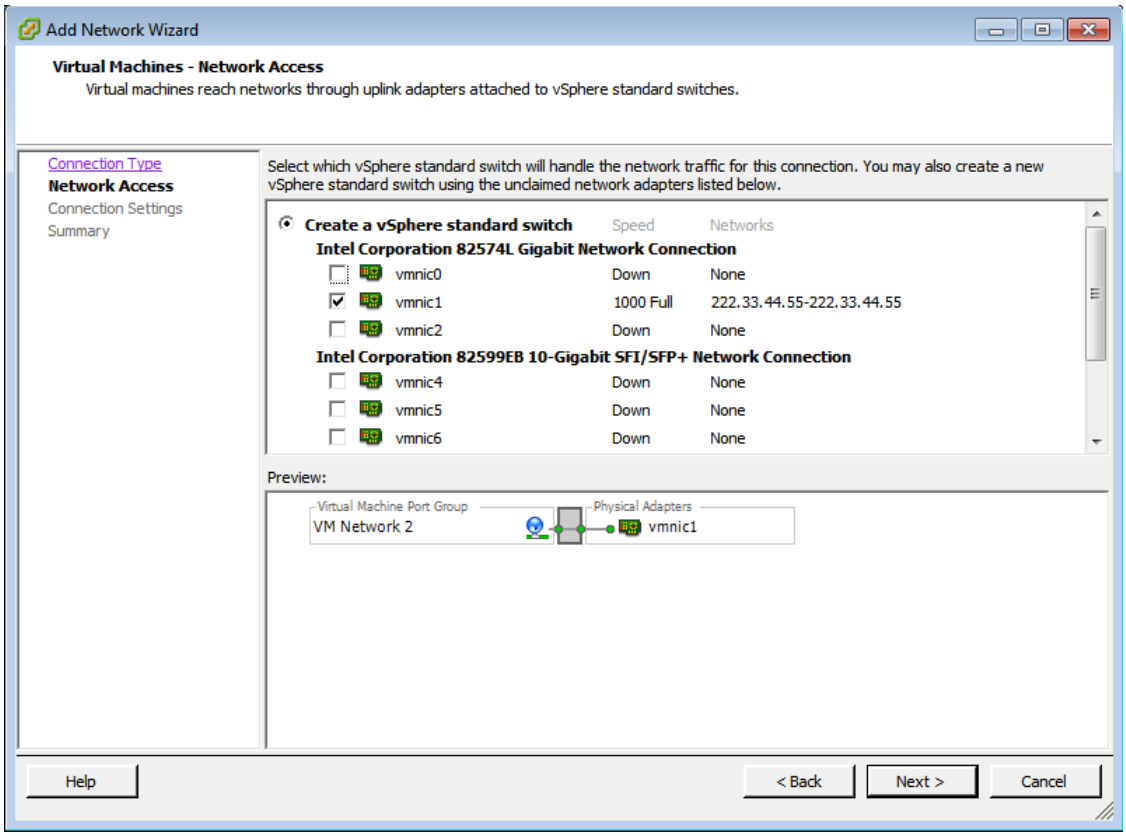

Рисунок 9. Указание физического сетевого адаптера для создания сети

2.6 На следующей странице **Connection Settings** укажите название создаваемой сети.

2.7 Проверьте, что созданная сеть закреплена за физическим адаптером, который вы выбрали на шаге 1. Для завершения настройки нажмите кнопку **Finish**.

3 На вкладке **Configuration** убедитесь, что созданный виртуальный коммутатор сопоставлен необходимому физическому сетевому адаптеру, выбранному на шаге 1.

4 В свойствах созданного виртуального коммутатора включите для него режим **Promiscuous mode**, позволяющий принимать все пакеты, независимо от того, кому они предназначены. Для этого:

4.1 На вкладке **Configuration** выберите созданный виртуальный коммутатор и щелкните **Properties**.

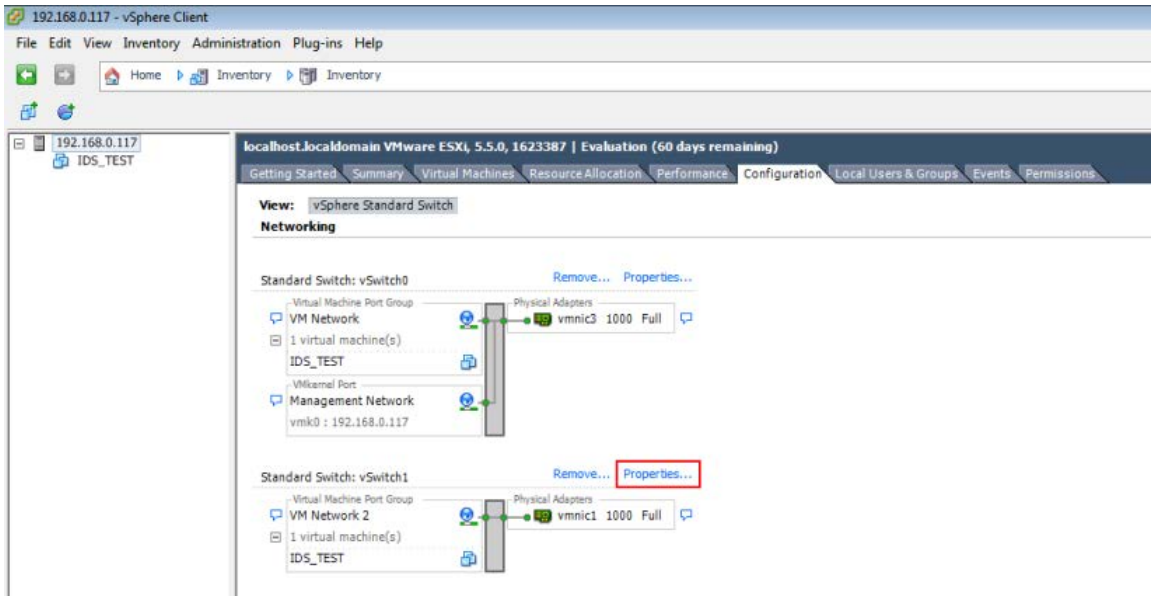

Рисунок 10. Просмотр свойств созданного виртуального коммутатора

4.2 В открывшемся окне **Properties** выберите вкладку **Security** и в списке **Promiscuous Mode** выберите **Accept**.

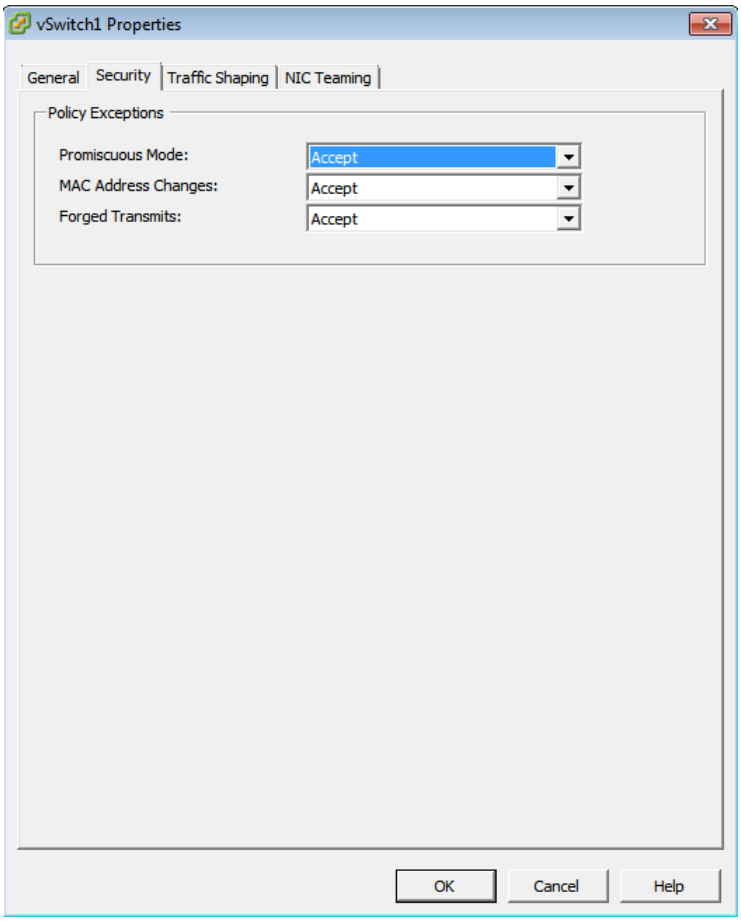

Рисунок 11. Включение режима Promiscuous mode

5 В настройках виртуальной машины с развернутым образом ViPNet IDS VA для одного из сетевых адаптеров, который будет выполнять функции интерфейса захвата трафика, выберите

в качестве сети подключения созданную виртуальную сеть. Данная настройка позволит интерфейсу захвата получать трафик локальных сетей от коммутатора со SPAN-портом. Для этого:

5.1 В левой панели выберите виртуальную машину и в контекстном меню по правой кнопке мыши нажмите **Edit Settings**.

5.2 В открывшемся окне **Virtual Machine Properties** на вкладке **Hardware** щелкните нужный сетевой адаптер и в списке **Network label** выберите имя созданной виртуальной сети.

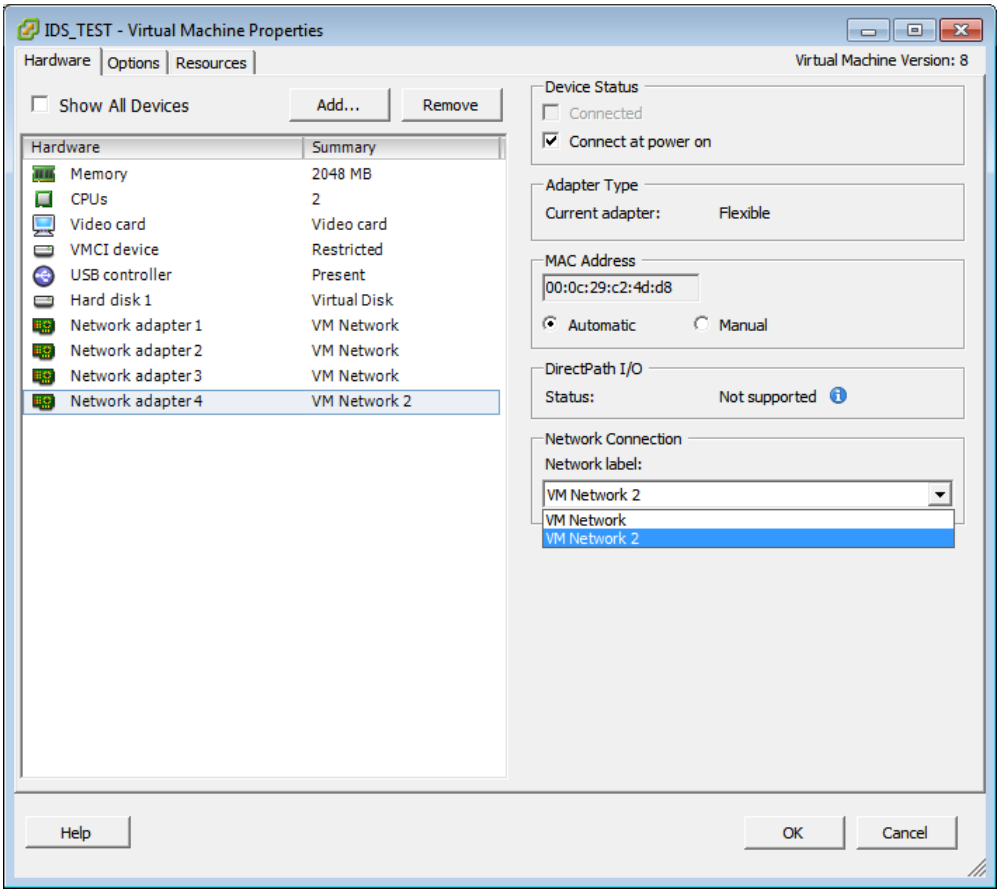

Рисунок 12. Выбор созданной виртуальной сети в качестве типа сетевого подключения для адаптера виртуальной машины

В результате будет сконфигурирован сетевой интерфейс захвата трафика, на который будет передаваться весь сетевой трафик локальной сети, зеркалируемый на ViPNet IDS SPAN-портом.

Далее запустите ViPNet IDS VA, смените пароль администратора системы, заданный по умолчанию, и проверьте, что настроенный сетевой адаптер не является управляющим интерфейсом. Для этого:

1. Запустите IDS Консольный конфигуратор.
2. В главном окне IDS-конфигуратора перейдите в раздел **IP Адреса** и убедитесь, например, сравнив MAC-адреса, что настроенный в пункте 5 сетевой адаптер не выбран в качестве управляющего интерфейса.

Подробнее см. документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора».

Настройки подключения для организации анализа трафика виртуальной локальной сети

Схема подключения ViPNet IDS VA для анализа сетевого трафика виртуальной локальной сети представлена ниже.

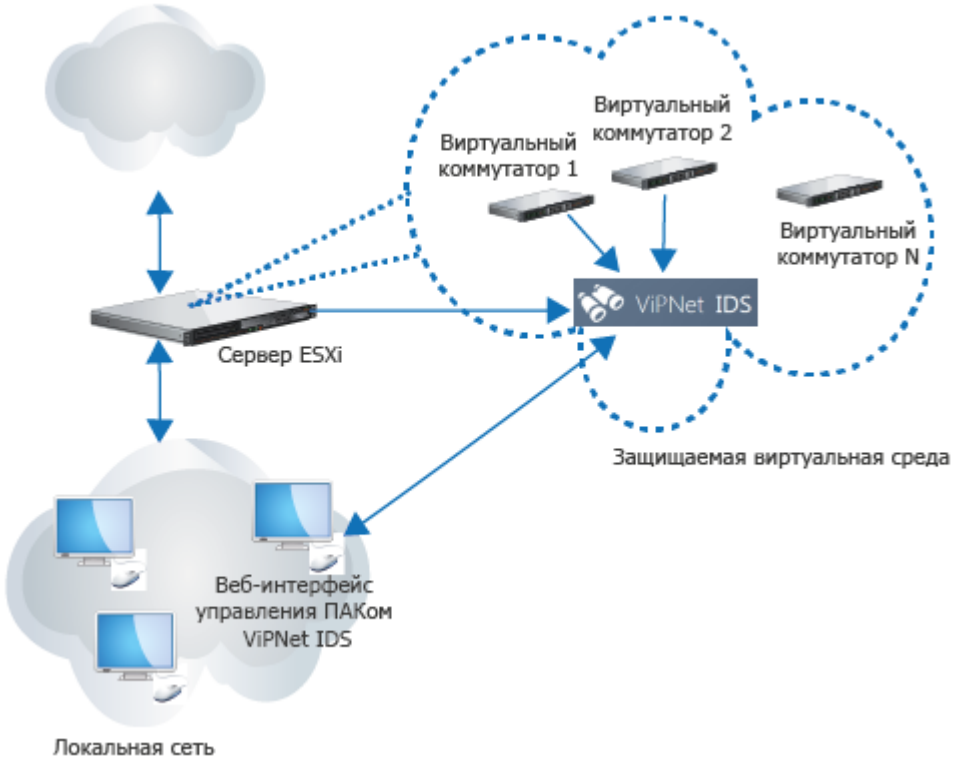

Рисунок 13. Схема подключения ViPNet IDS VA для организации анализа сетевого трафика виртуальных локальных сетей

Если у вас имеется несколько стандартных виртуальных сетевых коммутаторов (standard switches), подключенных к различным виртуальным локальным сетям, для возможности анализа трафика от этих локальных сетей необходимо для каждого соответствующего виртуального коммутатора на VIPNet IDS закрепить и настроить интерфейс захвата трафика, на который будет передаваться трафик соответствующей виртуальной сети.

Примечание. В случае использования распределенного виртуального сетевого коммутатора (distributed switch) анализ трафика соответствующей виртуальной сети производиться не будет в связи с невозможностью настроить режим **Promiscuous mode** для сетевого коммутатора такого типа.

Для настройки интерфейсов захвата выполните следующие действия:

1 Запустите программу VMware vSphere Client и подключитесь к серверу ESXi (vCenter Server).

2 В настройках виртуальной машины с развернутым образом ViPNet IDS VA для одного или нескольких (в зависимости от количества виртуальных сетей) сетевых адаптеров, которые будут выполнять функции интерфейсов захвата, выберите в качестве сети подключения существующую виртуальную сеть, трафик которой необходимо анализировать. Для этого:

2.1 В левой панели выберите виртуальную машину с ViPNet IDS и в контекстном меню по правой кнопке мыши нажмите **Edit Settings**.

2.2 В открывшемся окне **Virtual Machine Properties** на вкладке **Hardware** щелкните один из сетевых адаптеров и в списке **Network label** выберите имя виртуальной сети, трафик которой необходимо анализировать.

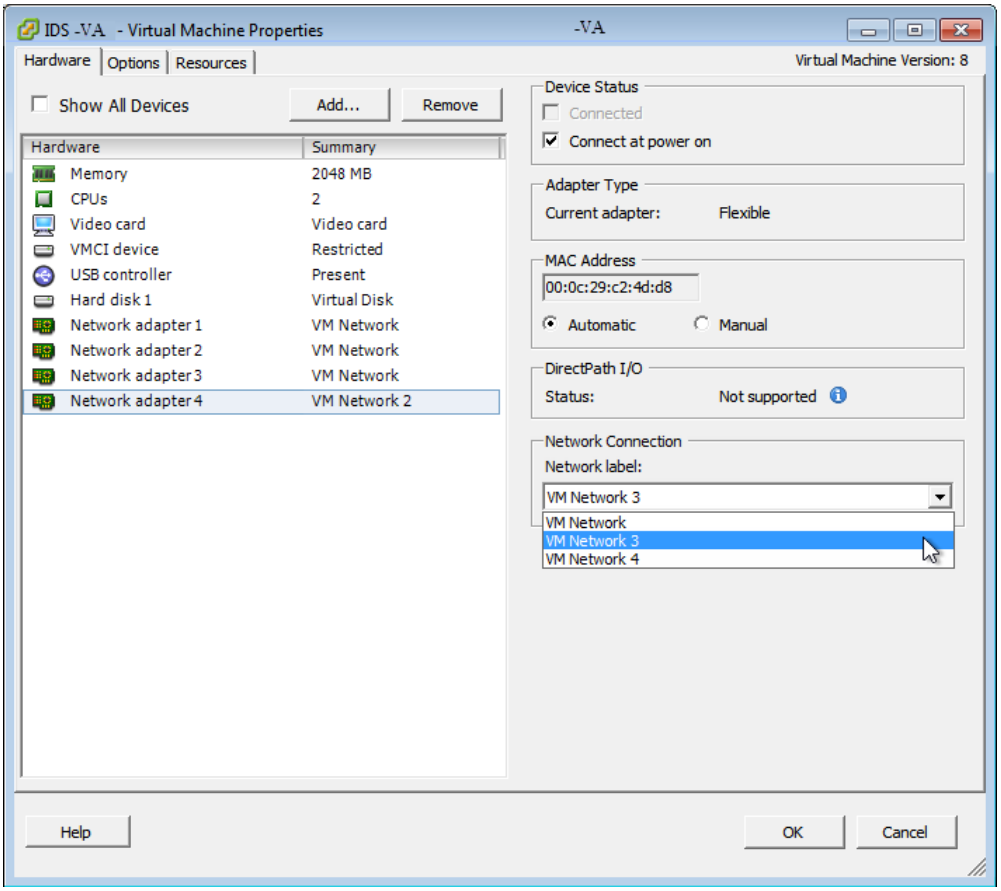

Рисунок 14. Выбор виртуальной сети в качестве типа сетевого подключения для адаптера виртуальной машины

3 В свойствах виртуального коммутатора для каждой виртуальной сети, трафик которой необходимо анализировать, включите режим **Promiscuous mode**, позволяющий принимать все пакеты, независимо от того, кому они предназначены. Для этого:

3.1 На вкладке **Configuration** выберите нужный виртуальный коммутатор и щелкните **Properties**.

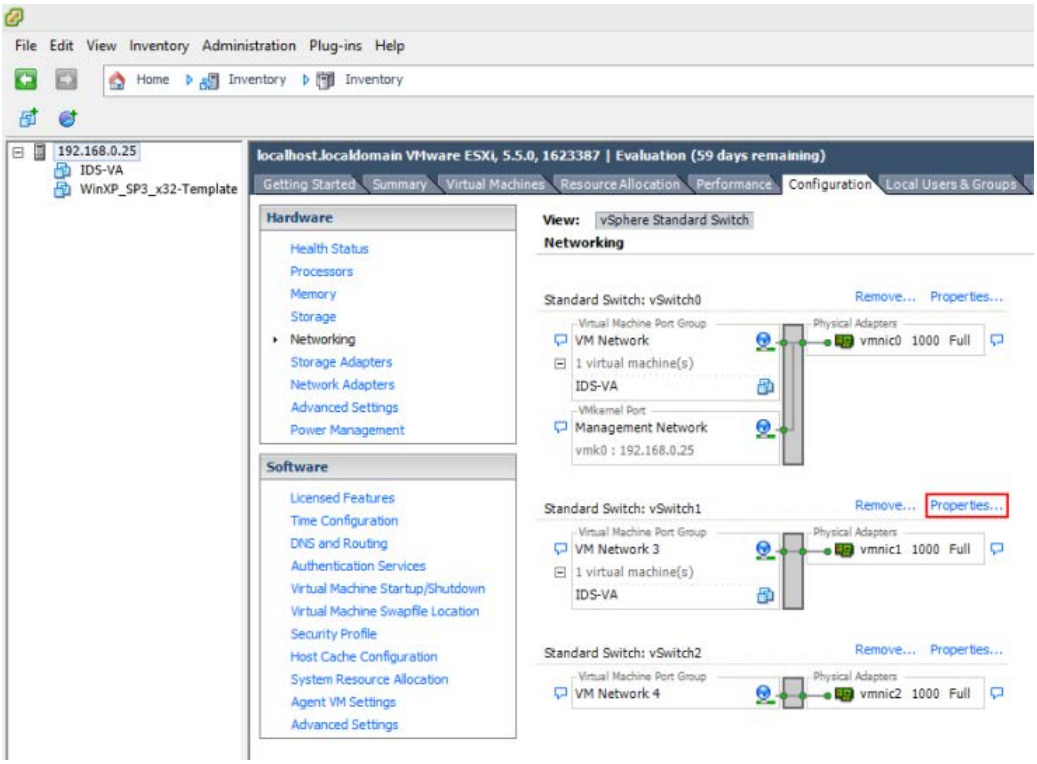

Рисунок 15. Просмотр свойств виртуального коммутатора, трафик которой необходимо анализировать

3.2 В открывшемся окне **Properties** выберите вкладку **Security** и в списке **Promiscuous Mode** выберите **Accept**.

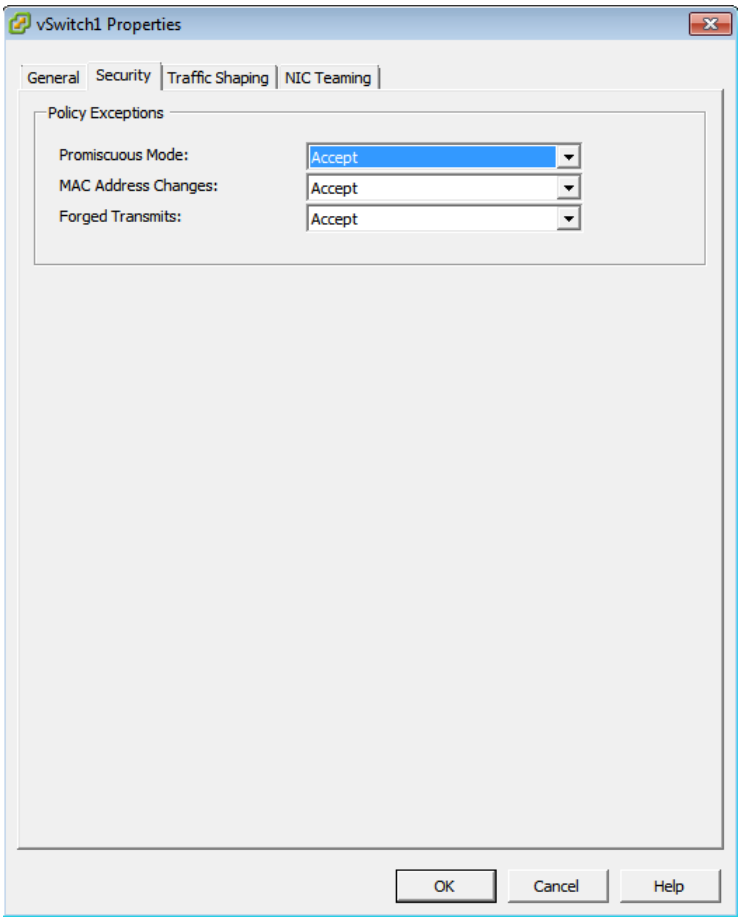

Рисунок 16. Включение режима Promiscuous mode

В результате будут сконфигурированы сетевые интерфейсы захвата трафика, на которые будет передаваться весь сетевой трафик от соответствующих виртуальных сетей.

Далее запустите ViPNet IDS VA, смените пароль администратора системы, заданный по умолчанию, и проверьте, что настроенные сетевые адаптеры ViPNet IDS не являются управляющим интерфейсом. Для этого:

1. Запустите IDS Консольный конфигуратор.
2. В главном окне IDS-конфигуратора перейдите в раздел **IP Адреса** и убедитесь, например, сравнив MAC-адреса, что настроенные в пункте 2 сетевые адаптеры не выбраны в качестве управляющего интерфейса.

Подробнее см. документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора».

Настройки подключения комбинированного варианта

Схема подключения ViPNet IDS VA для анализа сетевого трафика физической и виртуальной локальных сетей представлена ниже.

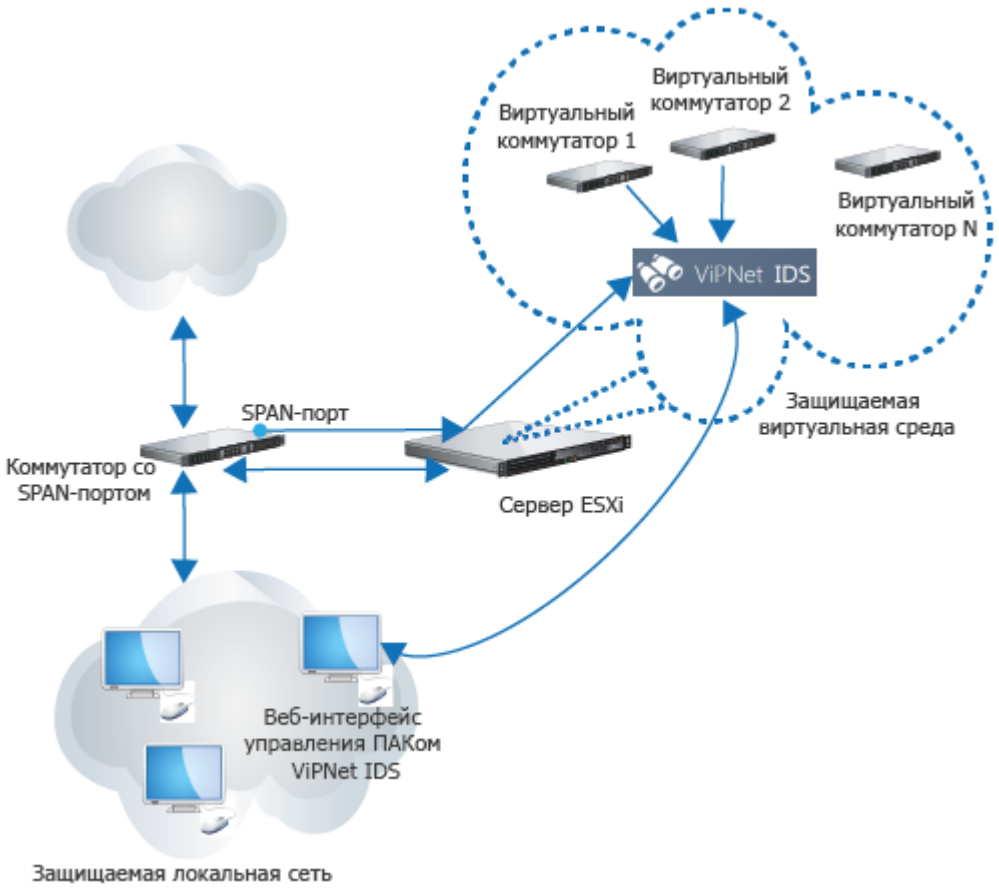

Рисунок 17. Схема подключения ViPNet IDS VA для анализа сетевого трафика физической и виртуальных локальных сетей

Для настройки интерфейсов захвата трафика для данного варианта необходимо произвести все настройки, указанные в разделах Настройки подключения для организации анализа трафика виртуальной локальной сети (на стр. 25) и Настройки подключения для организации анализа трафика физической локальной сети (на стр. 19).

Создание запроса на лицензию

Для получения лицензии на использование ViPNet IDS VA необходимо создать файл с запросом на лицензию и отправить его в отдел технического сопровождения ОАО «ИнфоТеКС», отвечающий за лицензирование.

Чтобы создать файл с запросом на лицензию, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet IDS под учетной записью главного администратора.
2. В верхнем правом углу веб-интерфейса в меню **Справка** выберите пункт **О продукте**.
3. Нажмите кнопку **Создать файл с запросом на лицензию** и укажите место сохранения файла.

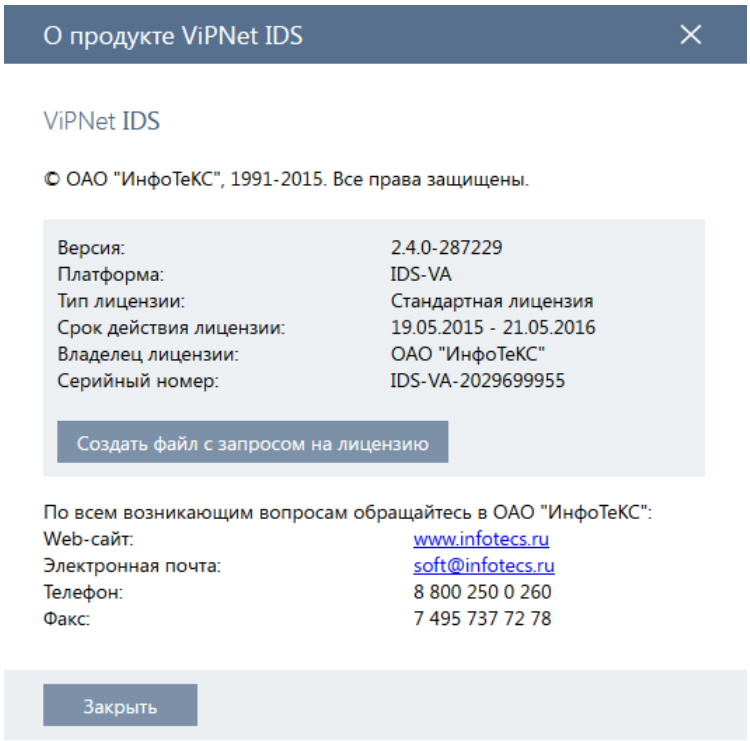

Рисунок 18. Создание файла с запросом на лицензию

В результате в указанной папке будет сохранен файл `sysid`, содержащий запрос на лицензию. Передайте файл с запросом в отдел технического сопровождения ОАО «ИнфоТеКС», отвечающий за лицензирование, для формирования файла лицензии.

После получения файла лицензии установите лицензию на ViPNet IDS (см. документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Установка лицензии на ViPNet IDS»).

4

Обновление ViPNet IDS

Порядок действий

Для обновления ПО ViPNet IDS VA вам необходимо будет заново установить виртуальный образ новой версии ViPNet IDS VA, выполнить ряд настроек, а затем восстановить из заранее сохраненных резервных копий все существующие в предыдущей версии параметры и журналы событий.

При обновлении ViPNet IDS VA на версию 2.4.1 следует учитывать следующие особенности:

1. В связи с изменениями в работе исполнения ViPNet IDS VA после обновления до версии 2.4.1 необходимо будет получить новый файл лицензии.
2. В связи с тем, что в версии 2.4.1 введены ограничения доступа к консоли Linux, изменилось имя учетной записи администратора системы. В версии 2.4.1 администратор системы будет иметь имя учетной записи — `idsuser`. После установки версии 2.4.1 используйте для авторизации в консоли Linux новое имя учетной записи. Пароль по умолчанию не изменился — vipnet

Для обновления ПО ViPNet IDS VA выполните все действия из приведенного ниже списка.

Внимание! Перед обновлением ПО создайте резервные копии всех параметров ViPNet IDS и журналов событий, сохраните их на внешний носитель в соответствии с разделами «Создание резервной копии конфигурации ViPNet IDS» и «Создание резервной копии журналов событий и содержимого пакетов» документа «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора». Резервные копии необходимы для восстановления всех данных после обновления ViPNet IDS.

Примечание. Описание обновления ViPNet IDS VA приведено на примере платформы виртуализации VMware ESXi. Предполагается, что в сети уже развернут сервер ESXi (vCenter Server) и настроено подключение к нему клиентов VMware vSphere Client.

Таблица 4. Последовательность действий по обновлению ViPNet IDS VA

	Действие	Ссылка
☐	Установите виртуальный образ новой версии ViPNet IDS VA на платформу виртуализации	Установка ViPNet IDS VA на платформу виртуализации (на стр. 17)
☐	В зависимости от способа организации вашей сети и ваших потребностей по выявлению аномалий сетевого трафика сконфигурируйте сетевой интерфейс, который будет работать на ViPNet IDS как интерфейс захвата трафика	Конфигурирование интерфейсов захвата трафика (на стр. 19)
☐	Запустите ViPNet IDS VA. При первом запуске смените пароль администратора системы, заданный по умолчанию	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Первый запуск ViPNet IDS. Смена пароля администратора системы»
☐	Произведите настройку управляющего интерфейса в IDS Консольном конфигураторе	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Изменение настроек управляющего интерфейса ViPNet IDS»
☐	Задайте часовой пояс и системное время на ViPNet IDS в IDS Консольном конфигураторе	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Задание системного времени и часового пояса на ViPNet IDS»
☐	Подключитесь к веб-интерфейсу ViPNet IDS для дальнейших настроек ViPNet IDS и смените пароль по умолчанию для главного администратора	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Подключение к веб-интерфейсу ViPNet IDS и завершение работы с ним» и раздел «Смена пароля главного администратора при первом подключении к веб-интерфейсу»
☐	Создайте файл с запросом на новую лицензию ViPNet IDS и отправьте его в отдел технического сопровождения ОАО «ИнфоТеКС», отвечающий за лицензирование	Создание запроса на лицензию (на стр. 30)
☐	После получения лицензии установите ее на ViPNet IDS	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Установка лицензии на ViPNet IDS»

	Действие	Ссылка
☐	Восстановите конфигурацию ViPNet IDS из резервной копии	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Восстановление конфигурации ViPNet IDS»
☐	В консоли Linux с помощью IDS Консольного конфигуратора восстановите журналы событий из резервной копии	Документ «Программно-аппаратный комплекс ViPNet IDS. Руководство администратора» раздел «Восстановление журналов событий и содержимого пакетов»
☐	Создайте SnapShot виртуальной машины, который может потребоваться вам для восстановления виртуальной машины в случае сбоя.	В соответствии с документацией к используемой виртуальной среде

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

A

Глоссарий

IDS

Система обнаружения атак (вторжений), предназначенная для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS). Обеспечивает дополнительный уровень защиты компьютерных систем.

Используется для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

SPAN-порт

SPAN-порт (Switch Port Analyzer) позволяет зеркалировать (дублировать) трафик от одного или нескольких портов на отдельно взятый порт.

Виртуальная сеть

Объединяет виртуальные сетевые адаптеры виртуальных машин в виртуальную компьютерную сеть и определяется уникальной меткой. Могут быть служебными (VMkernel Port) и общего назначения (Virtual Machine Port group). Виртуальные сети общего назначения используются для передачи данных между виртуальными машинами, виртуальными машинами и внешней средой. Служебные виртуальные сети предназначены для управления виртуальной средой и/или передачи служебных данных.

Виртуальная среда

Это некоторая среда, где все виртуальное, то есть физически не существующее: виртуальные компьютеры (виртуальные машины), виртуальные компьютерные сети, виртуальные коммутаторы.

Виртуальный коммутатор

Это некоторое абстрактное устройство, которое передает данные между виртуальными машинами посредством виртуальных компьютерных сетей и осуществляет связь с внешним миром. Могут использоваться для балансировки сетевого трафика между физическими сетевыми адаптерами сервера.

Интерфейс захвата трафика

Сетевой интерфейс ПАК ViPNet IDS, на который передается весь сетевой трафик, зеркалируемый на ViPNet IDS SPAN-портом, для его дальнейшего анализа на предмет наличия атак.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Ответвитель трафика TAP

Аппаратное устройство, подсоединяемое непосредственно к кабелю компьютерной сети и передающее копию сетевого трафика другому устройству.

Сетевая атака

Попытка злоумышленника вывести узел из строя, например, в случае DoS-атаки (от англ. Denial of Service, отказ в обслуживании), или получить несанкционированный доступ в сеть с целью изменить, удалить данные или добавить нежелательные данные. Успех атаки зависит от степени уязвимости системы защиты и предпринимаемых контрмер.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве

физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Управляющий интерфейс

Сетевой интерфейс ViPNet IDS, к которому подключается компьютер для управления ViPNet IDS посредством веб-интерфейса.

Указатель