SBSS

Использование *ssProxy* в защищенных сетях

Москва 2008

СОДЕРЖАНИЕ

1 РЕПЛИКАЦИЯ В ЗАЩИЩЕННЫХ СЕТЯХ

В феврале 2007г. вступил в силу Федеральный закон № 152-ФЗ «О персональных данных». Этот факт дал разработчикам информационных систем дополнительный мощный стимул к использованию в своих разработках программных и аппаратных систем защиты информации от несанкционированного доступа.

1.1 *Суть проблемы*

На Рис.1-1 представлен простейший вариант размещения компонент «*SBSS*» в незащищенной сети.

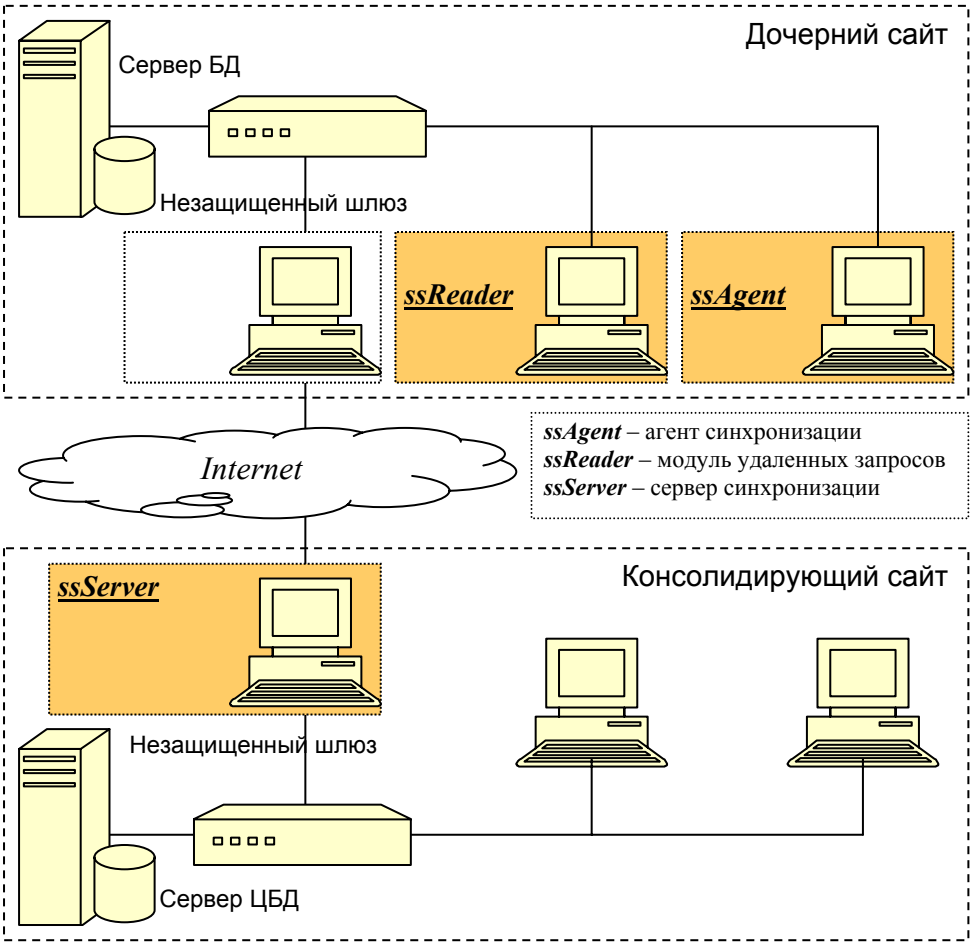


Рис.1-1 Незащищенная сеть

В консолидирующем сайте установлен сервер синхронизации *ssServer*, имеющий доступ к серверу баз данных. На рабочих станциях локальной сети дочерних сайтов установлены

- агент синхронизации *ssAgent*, выполняющий сеансы синхронизации базы данных дочернего и консолидирующего сайтов;
- модуль удаленных запросов *ssReader*, позволяющий с рабочих станций дочернего сайта выполнять запросы к базам данных консолидирующего сайта.

К достоинствам этого варианта топологии можно отнести следующее:

- простота реализации;
- сеансы синхронизации баз данных и удаленные запросы можно выполнять с любой рабочей станции дочернего сайта.

Основной недостаток этого варианта: отсутствуют средства защиты локальных сетей консолидирующего и дочернего сайтов, что делает возможным проведение атак со стороны публичной сети *Internet*.

Топология, представленная на Рис.1-2, иллюстрирует вариант размещения компонент «*SBSS*» в защищенной сети. Вообще говоря, для построения защищенных сетей могут использоваться различные программные и аппаратные комплексы (например, *VipNet* от ОАО «Инфотекс», *Заслон* от ЗАО «Голлард», *Дионис* от «Фактор-ТС» и др.). В данном случае, с целью внесения некоторой доли конкретики, мы будем иллюстрировать суть проблемы на примере защищенной сети, построенной на основе программного комплекса *VipNet*. *VipNet* позволяет организовать защищенные туннели через публичную сеть *Internet*, чем достигается высокая степень защиты от внешних атак.

Защищенный туннель *VipNet* обеспечивается такими его компонентами, как «*VipNet-клиент*», «*VipNet-координатор*» и «*VipNet-администратор*». В рассматриваемом примере *VipNet-клиент* установлен на шлюзовом компьютере дочернего сайта. На шлюзе консолидирующего сайта установлен *VipNet-координатор*. *VipNet-администратор* размещен на одной из рабочих станций локальной сети консолидирующего сайта.

Достоинство представленного на Рис.1-2 варианта топологии очевидно: все межсетевые пакеты транслируются через защищенный туннель, что практически исключает возможность внешних атак. Однако подобный подход влечет за собой следующую проблему: межсетевое взаимодействие возможно лишь с защищенного компь-

ютера (шлюза) дочернего сайта. В большинстве случаев это нарушает нормальный технологический процесс обработки информации в дочернем сайте.

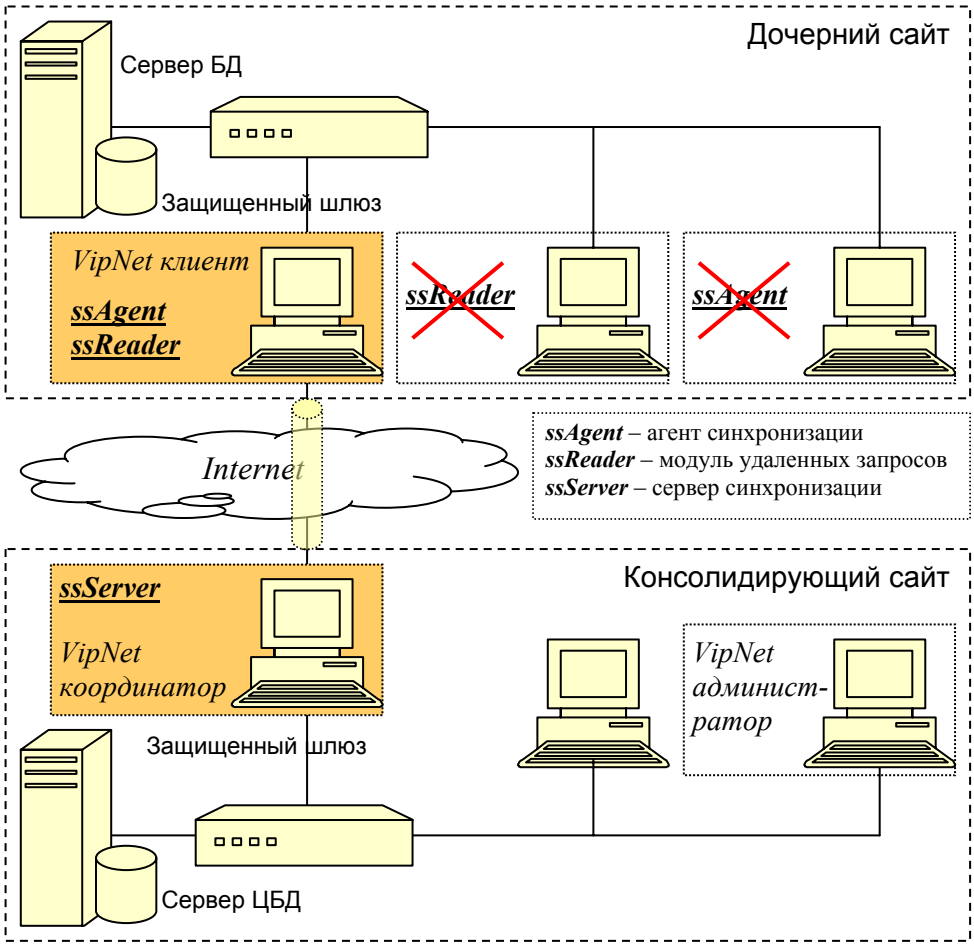


Рис.1-2 Защищенная сеть. Примитивный подход

Одно из возможных решений, представленное на Рис.1-3, состоит в установке *VipNet-клиента* на все компьютеры дочернего сайта.

Впрочем, такой вариант топологии защищенной сети также несет в себе ряд недостатков:

- требуется приобретение дополнительных лицензий на установку каждого *VipNet-клиента*;
- администратор защищенной сети должен выполнить комплекс работ по установке *VipNet-клиентов* в дочернем сайте, их конфигурированию и снабжению ключами с помощью *VipNet-администратора* в консолидирующем сайте.

Очевидно, что при большом количестве дочерних сайтов с развитыми локальными сетями, эти недостатки носят слишком серьезный характер.

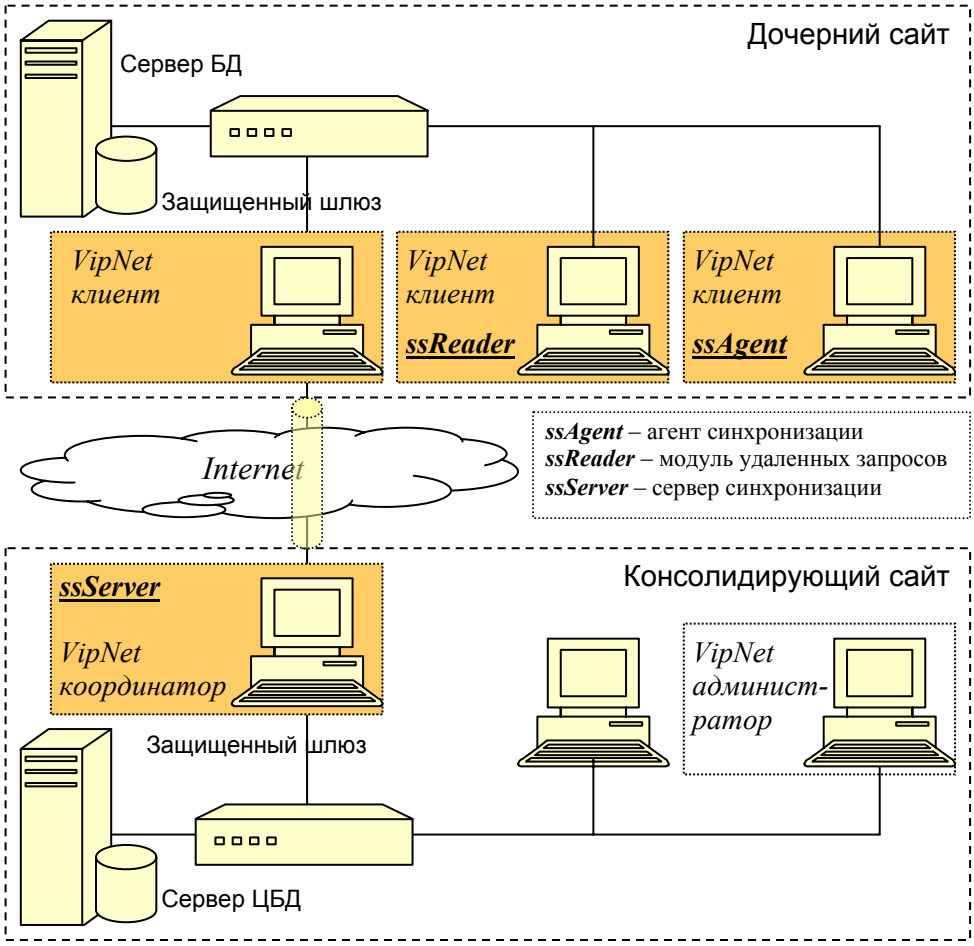


Рис.1-3 Защищенная сеть.

Вариант использования нескольких VipNet-клиентов в дочернем сайте

1.2 *Использование ssProxy*

Решение проблемы было найдено в разработке специального компонента сеансовой синхронизации *ssProxy*, выполняющего роль посредника (ретранслятора) между агентом синхронизации (модулем удаленных запросов) и сервером синхронизации.

Возможно использование следующих схем установки *ssProxy*:

- однозвенная схема (Рис.1-4);
- двухзвенная схема (Рис.1-5).

1.2.1 Однозвенная схема

Однозвенная схема предполагает использование *ssProxy* только в дочерних сайтах. При этом в звеньях информационных потоков строятся цепочки следующего вида:

ssAgent → *ssProxy_на_клиенте* → *ssServer*

ssReader → *ssProxy_на_клиенте* → *ssServer*

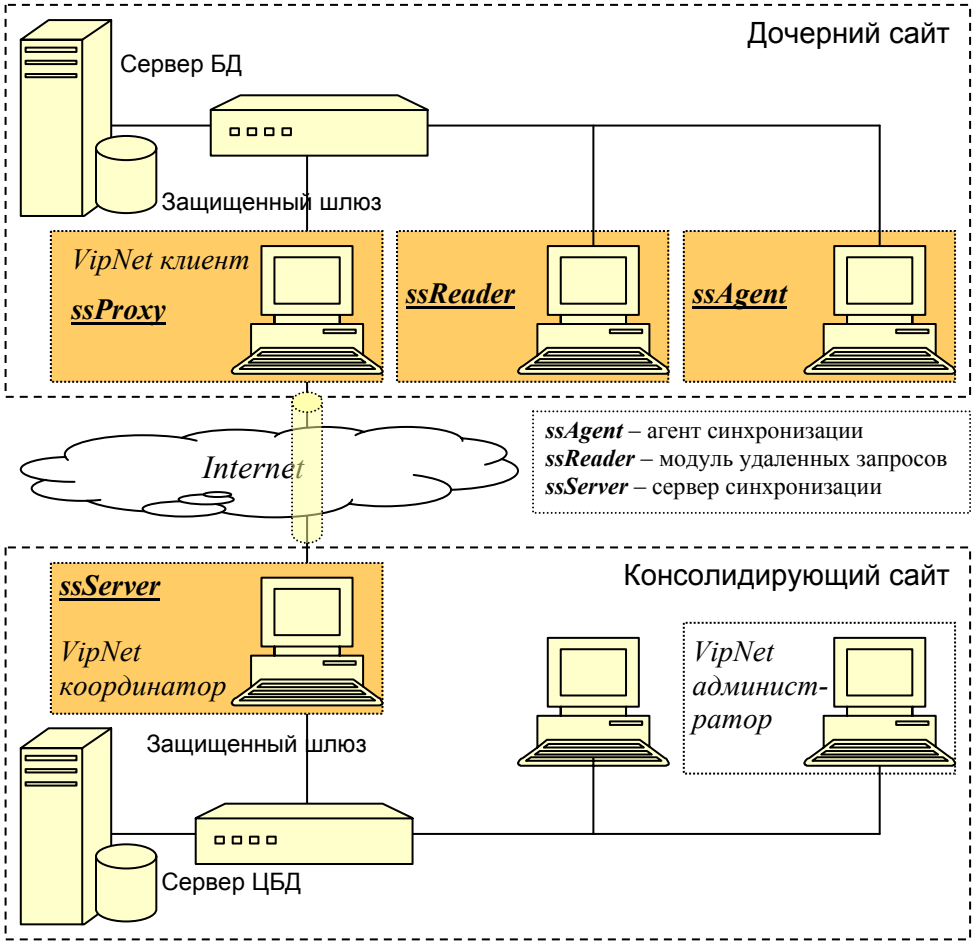


Рис.1-4 Защищенная сеть. Однозвенная схема установки ssProxy

Типовая однозвенная схема установки *ssProxy* представлена на Рис.1-4. В этой схеме информационный обмен через публичную сеть *Internet* осуществляется через защищенный туннель, формируемый между *VipNet*-шлюзами (*VipNet-клиентом* дочернего сайта и *VipNet–координатором* консолидирующего сайта).

1.2.2 Двухзвенная схема

Двухзвенная схема предполагает использование *ssProxy* в дочерних сайтах и в консолидирующем сайте. При этом в звеньях информационных потоков строятся цепочки следующего вида:

ssAgent → *ssProxy_на_клиенте* → *ssProxy_на_сервере* → *ssServer*

ssReader → *ssProxy_на_клиенте* → *ssProxy_на_сервере* → *ssServer*

Типовая двухзвенная схема установки *ssProxy* представлена на Рис.1-5.

В отличие от первого варианта, в этой схеме сервер синхронизации, имеющий доступ к серверам баз данных консолидирующего сайта, скрывается за *VipNet-координатором* (защищенным шлюзом) консолидирующего сайта.

В обеих схемах рабочие станции дочерних сайтов, на которых установлены агент синхронизации (*ssAgent*) и модуль удаленных запросов (*ssReader*), не имеют выхода в *Internet*, т.е. не могут взаимодействовать непосредственно с сервером синхронизации (*ssServer*) консолидирующего сайта. Связующим звеном в этом случае служит *ssProxy*. Он выполняет роль посредника (ретранслятора) между *ssAgent/ssReader* и *ssServer*, осуществляя трансляцию сетевых пакетов между ними.

Применение *ssProxy* для решения задачи синхронизации распределенных баз данных в защищенных сетях позволяет решить целый комплекс проблем. При этом *ssProxy* отличается простотой установки, исключает затраты на лицензирование и не требует дополнительного администрирования сайтов распределенной системы.

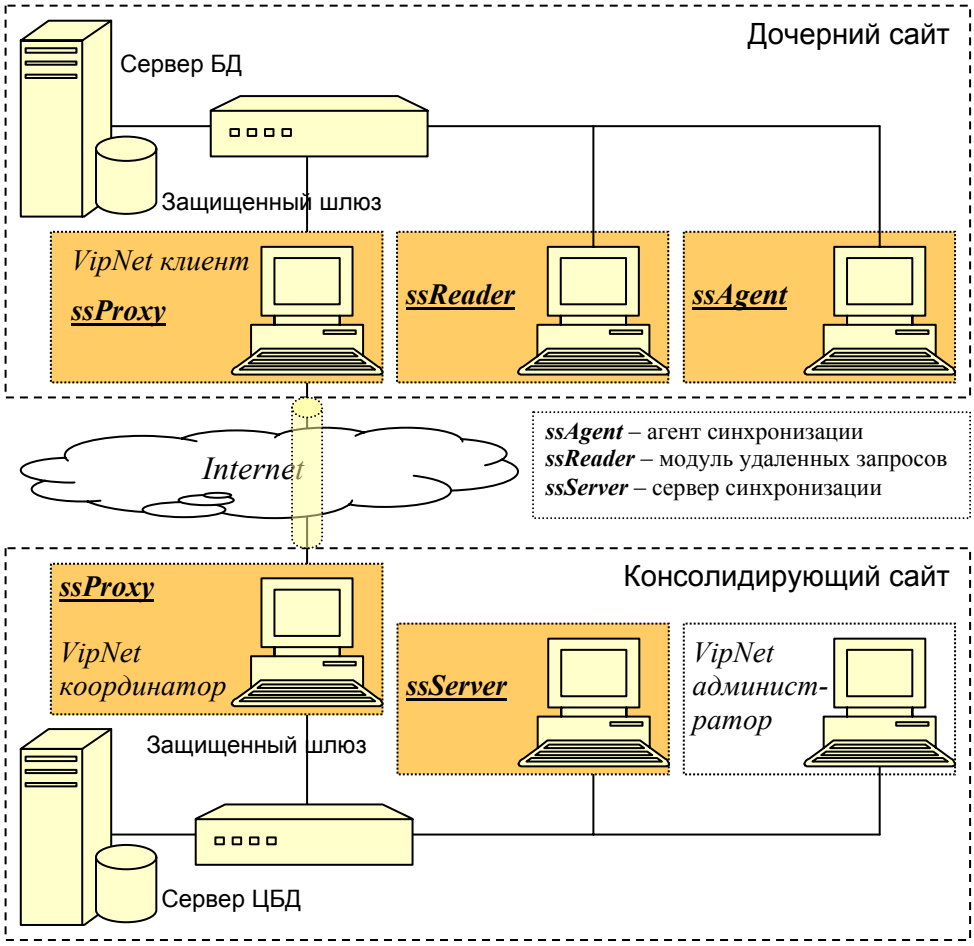


Рис.1-5 Защищенная сеть. Двухзвенная схема установки ssProxy

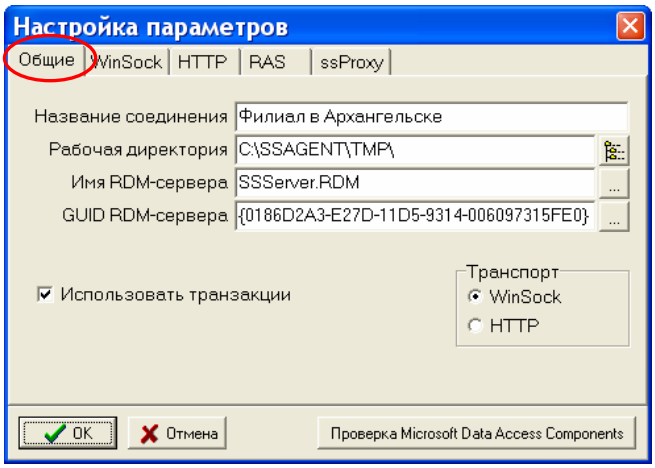
1.3 *Настройка ssAgent и ssReader для работы с ssProxy*

Обычно для взаимодействия *ssProxy* с агентом синхронизации (*ssAgent*) и модулем удаленных запросов (*ssReader*) внутри ЛВС дочерних сайтов применяется протокол *WinSock*. Это предполагает возможность использования библиотеки перехвата, осуществляющей сжатие и распаковку сетевых пакетов, передаваемых между компонентами системы сеансовой синхронизации.

Собственно настройка заключается в задании параметров внешних соединений для агента синхронизации и модуля удаленных запросов.

Агент синхронизации и модуль удаленных запросов настраиваются идентично.

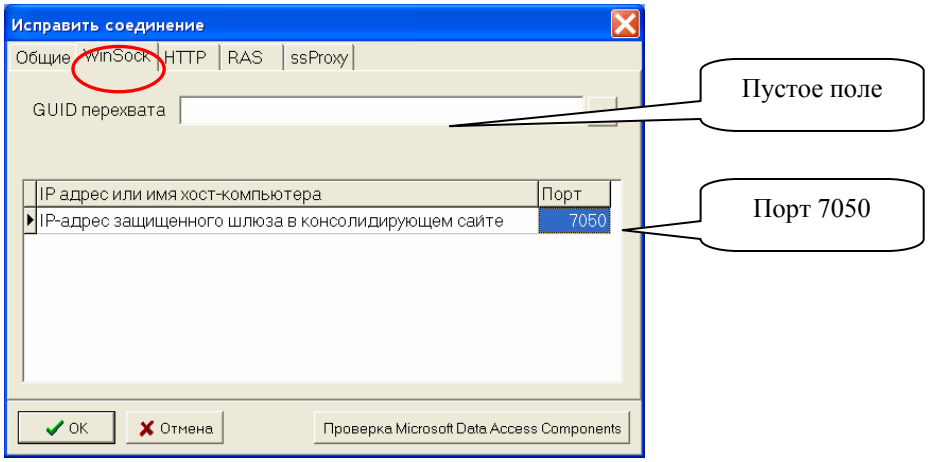
На закладке «*Общие*» диалогового окна настройки в поле «*Название соединения*» введите название дочернего сайта и информационного потока:



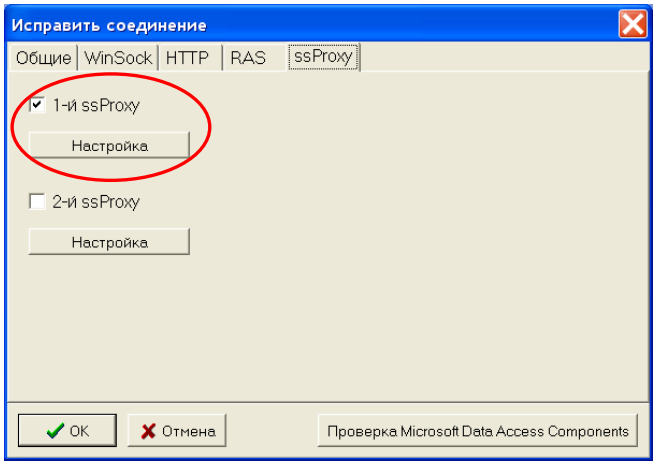
Если сжатие сетевого трафика не используется

Однозвенная схема

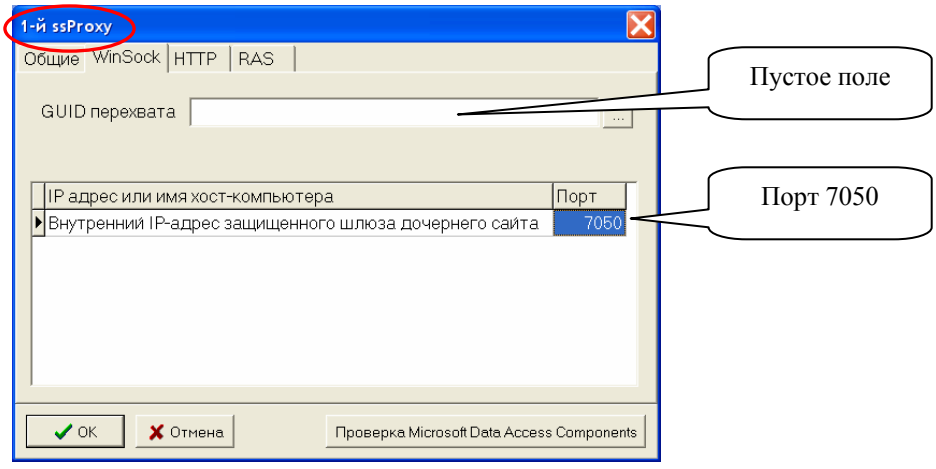
На закладке «*WinSock*» задается адрес конечного звена в цепочке (адрес компьютера с сервером синхронизации). В данном случае он установлен на защищенном шлюзе консолидирующего сайта:



Закладка «*ssProxy*»:



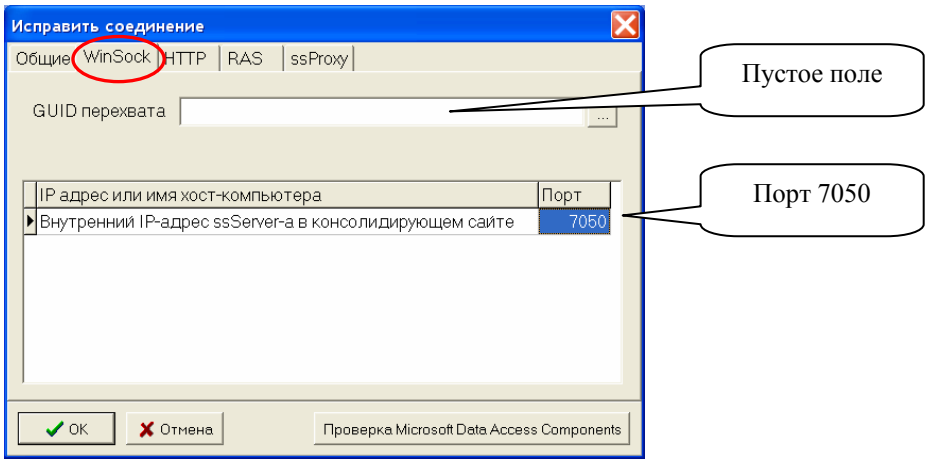
Нажмите кнопку «*Настройка*» под переключателем «*1-й ssProxy*».



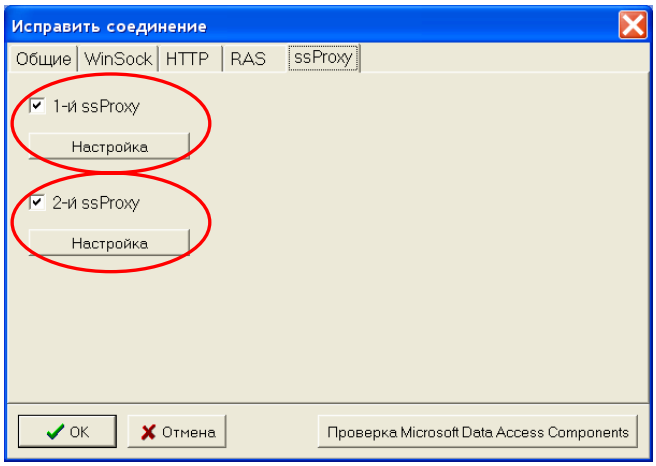
Очистьте поле «*GUID перехвата*», введите внутренний *IP*-адрес защищенного шлюза дочернего сайта, в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

Двухзвенная схема

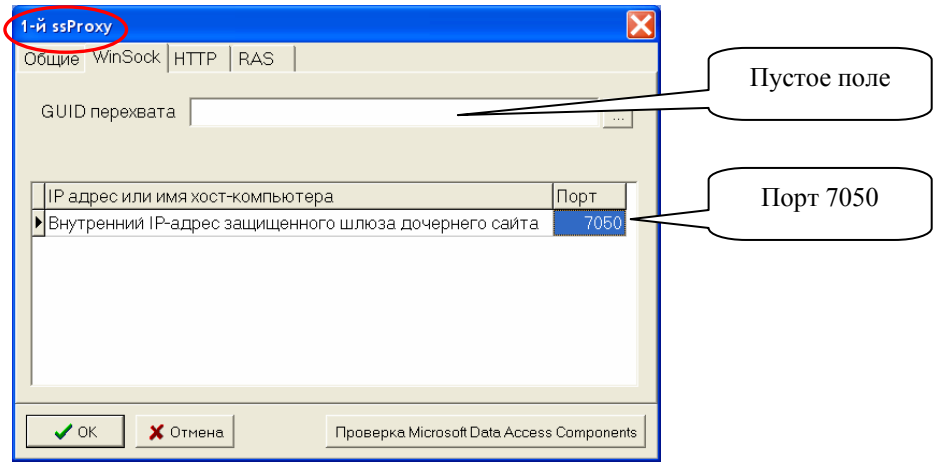
На закладке «*WinSock*» задается адрес конечного звена в цепочке (адрес компьютера с сервером синхронизации). В данном случае он установлен внутри локальной сети консолидирующего сайта:



Закладка «*ssProxy*»:

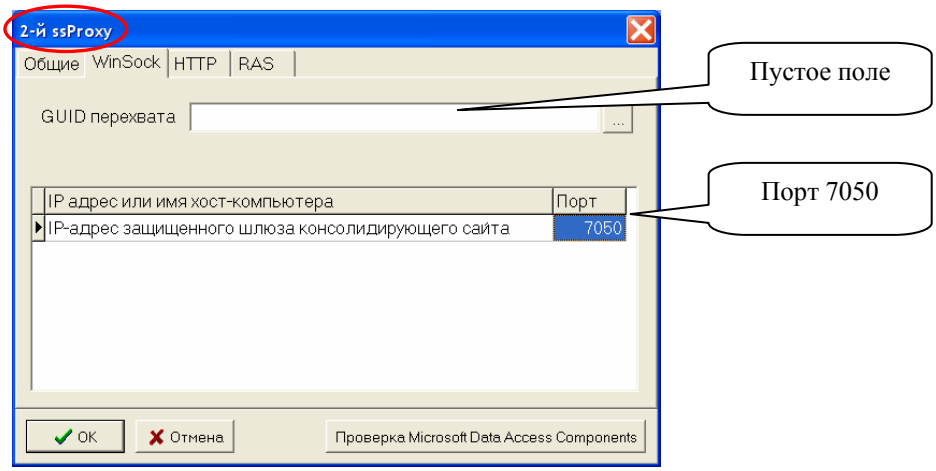


Нажмите кнопку «*Настройка*» под переключателем «*1-й ssProxy*».



Очистьте поле «*GUID перехвата*», введите внутренний *IP*-адрес защищенного шлюза в ЛВС дочернего сайта, в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

Нажмите кнопку «*Настройка*» под переключателем «*2-й ssProxy*»:

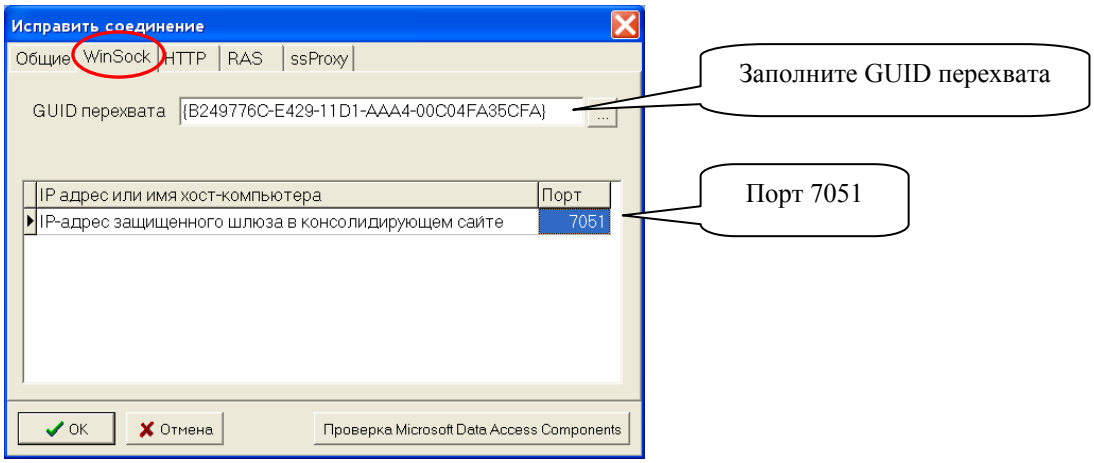


Очистьте поле «*GUID перехвата*», введите внешний *IP*-адрес защищенного шлюза консолидирующего сайта (где установлен 2-й *ssProxy*), в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

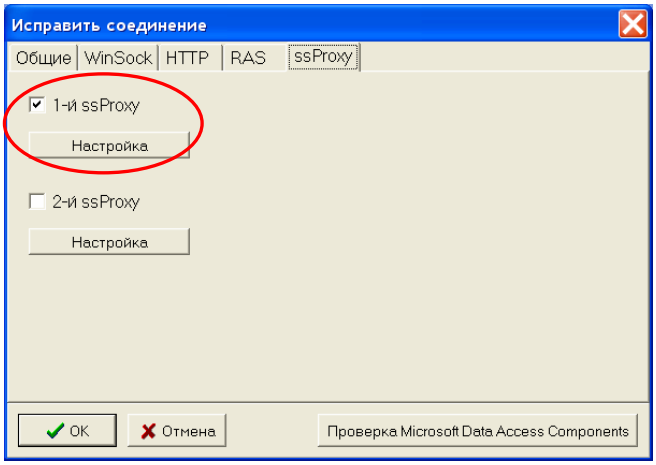
Если используется сжатие сетевого трафика

Однозвенная схема

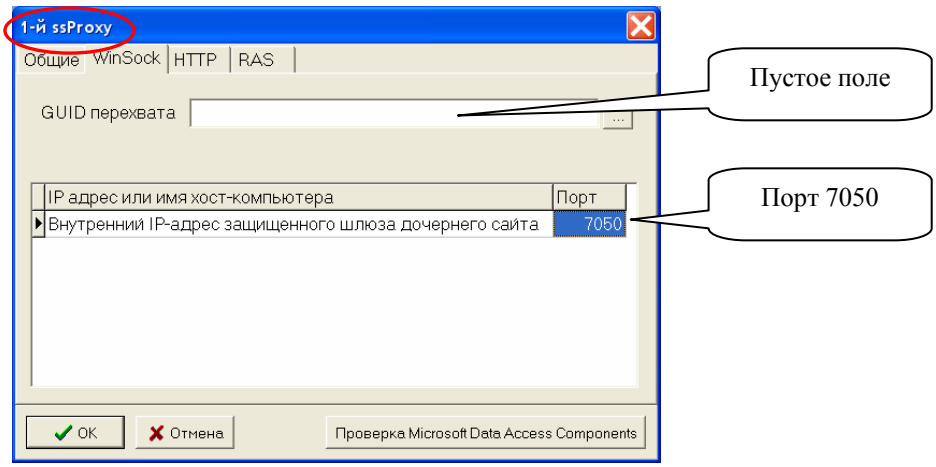
На закладке «*WinSock*» задается адрес конечного звена в цепочке (адрес компьютера с сервером синхронизации). В данном случае он установлен на защищенном шлюзе консолидирующего сайта:



Закладка «*ssProxy*»:



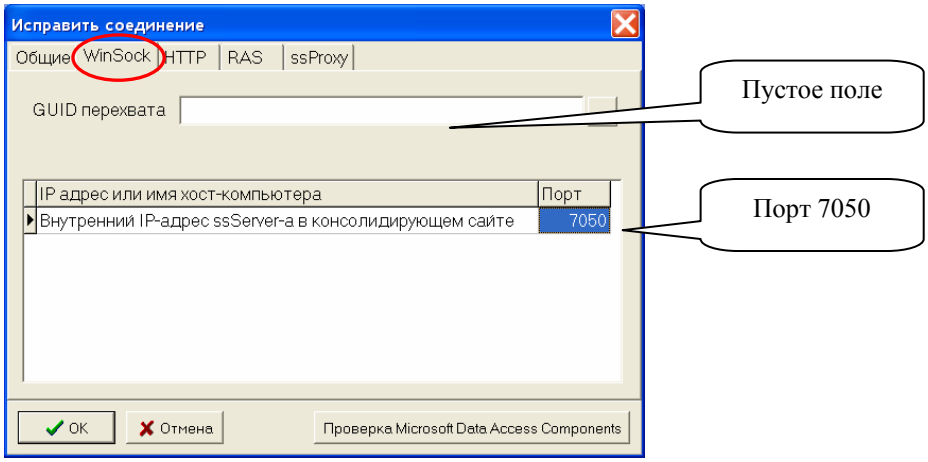
Нажмите кнопку «*Настройка*» под переключателем «*1-й ssProxy*».



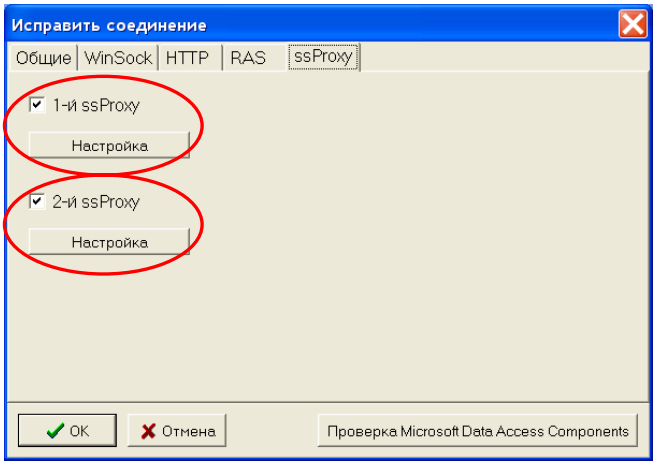
Очистьте поле «*GUID перехвата*», введите внутренний *IP*-адрес защищенного шлюза дочернего сайта, в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

Двухзвенная схема

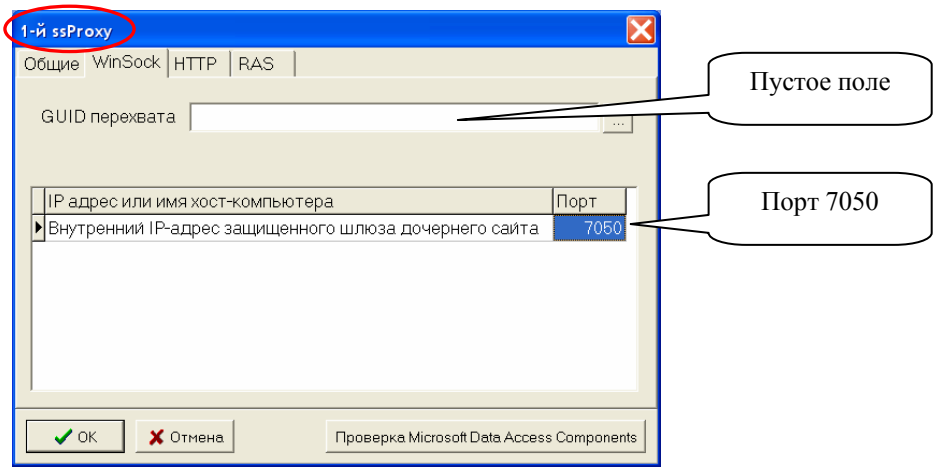
На закладке «*WinSock*» задается адрес конечного звена в цепочке (адрес компьютера с сервером синхронизации). В данном случае он установлен внутри локальной сети консолидирующего сайта:



Закладка «*ssProxy*»:

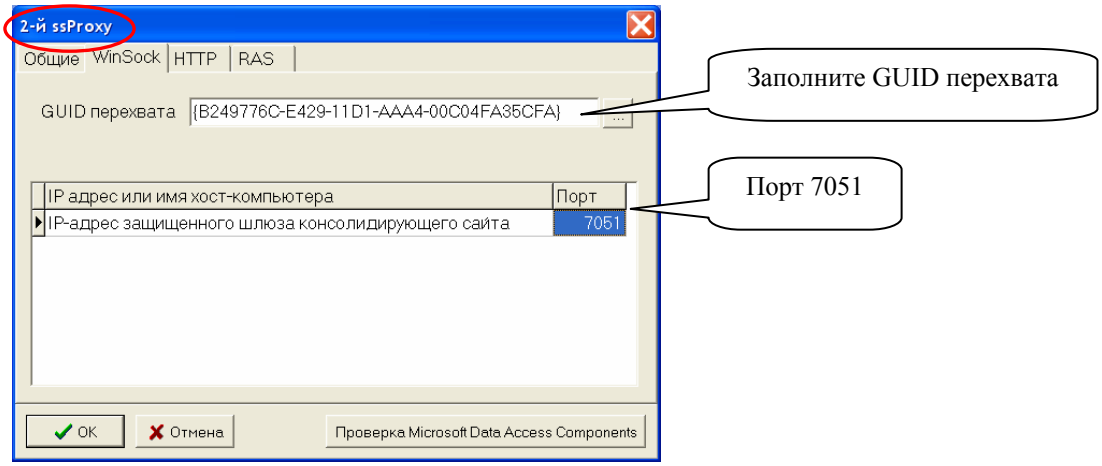


Нажмите кнопку «*Настройка*» под переключателем «*1-й ssProxy*».



Очистьте поле «*GUID перехвата*», введите внутренний *IP*-адрес защищенного шлюза в ЛВС дочернего сайта, в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

Нажмите кнопку «*Настройка*» под переключателем «*2-й ssProxy*»:



Заполните поле «*GUID перехвата*», введите внешний *IP*-адрес защищенного шлюза консолидирующего сайта (где установлен 2-й *ssProxy*), в качестве номера порта задайте значение «7050» и нажмите кнопку «*OK*».

Суть описанных выше настроек сводится к определению одного единственного коммуникационного звена, на котором будет использоваться библиотека перехвата, выполняющая упаковку/распаковку сетевых пакетов. Во всех случаях это звено – публичная сеть *Internet*. Схематично это представлено на Рис.1-6. Использование библиотеки перехвата в остальных звеньях коммуникационных цепочек допустимо, однако пагубно сказывается на быстродействии сеансов обмена, поскольку приводит к избыточным операциям упаковки/распаковки сетевых пакетов.

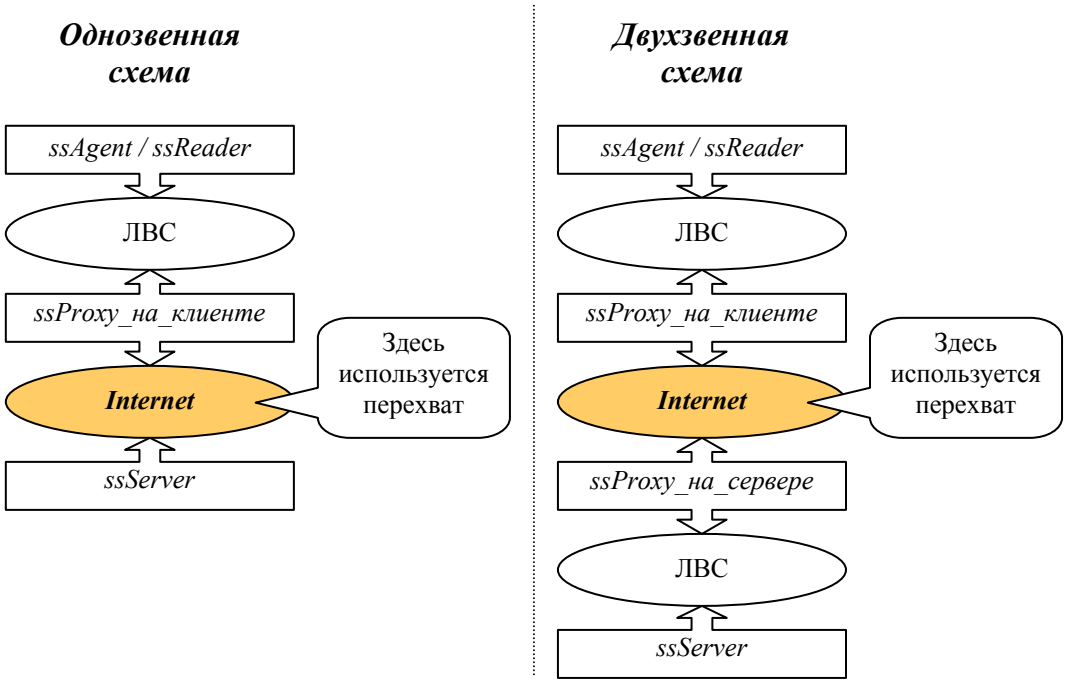


Рис.1-6 К определению звена для использования библиотеки перехвата

Помимо описанных схем на основе протокола *WinSock*, могут также применяться схемы на основе протокола *HTTP* и смешения протоколов *WinSock* и *HTTP* в одной цепочке. При этом обычно протокол *HTTP* применяется для прохождения публичной сети *Internet*, а протокол *WinSock* внутри ЛВС консолидирующих и дочерних сайтов (Рис.1-7).

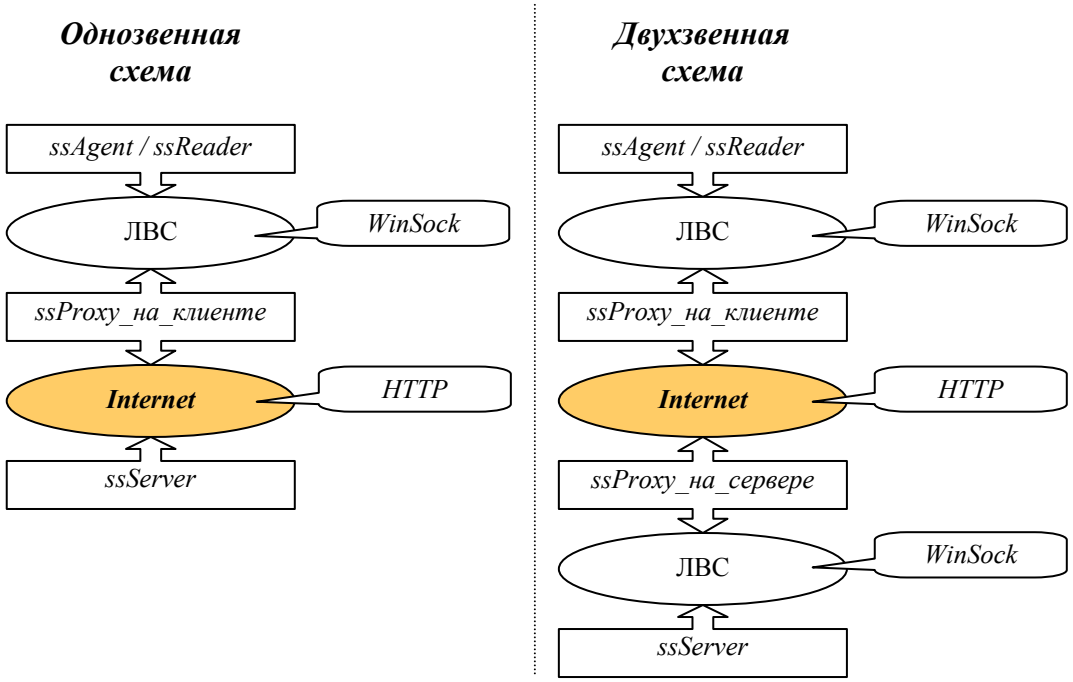


Рис.1-7 Смешение протоколов в различных схемах обмена

Применение протокола *WinSock* внутри локальных сетей предпочтительнее, поскольку, в отличие от протокола *HTTP*, не требует создания, настройки и администрирования *web*-сайтов на клиентской стороне. При использовании смешения протоколов, как это представлено на Рис.1-7, наличие *web*-сайта необходимо только на стороне консолидирующей базы данных.