

Настройка сервера ISA для работы с системой iBank 2

Руководство для корпоративных клиентов

Содержание

Введение	2
Принцип обработки запросов	3
Создание определения протоколов	5
Настройка правила протоколов	7
Создание правила протоколов	7
Изменение правила протоколов	9
Создание правила узлов и содержимого	11
Назначение подмножества адресатов для правила узлов и содержимого	12
Настройка фильтра IP-пакетов	14
Создание фильтра IP-пакетов	14
Настройка протокола для фильтра IP-пакетов	16
Применение фильтра IP-пакетов к серверу	17

Введение

Данный документ описывает процедуру настройки ISA (Internet Security Assistant) сервера для работы корпоративных клиентов с системой «iBank 2». ISA сервер предназначается для обеспечения информационной безопасности в сети организации. Его использование позволяет ограничить доступ из сети банковским сервером «iBank 2», запретив доступ с прочих IP адресов. Кроме того, ISA сервер позволяет контролировать номера портов, на которые разрешены или запрещены соединения, используемые протоколы, а также содержимое поступающих пакетов.

Ниже подробно рассмотрены как конфигурация созданного ISA сервера, так и настройка уже существующего.

- Отключить правила протоколов, запрещающие пересылку HTTPS запросов и запросов на порт 9091.
- Создать правило протоколов, разрешающее пересылку HTTPS запросов и запросов на порт 9091.
- Проверить правила узлов на наличие запрета доступа к банку.
- Создать правило узлов, разрешающее пересылку запросов.
- Проверить фильтрацию IP адресов.

Подробно данные действия описаны в соответствующих разделах ниже.

Создание определения протоколов

Для создания определения протокола выполните следующие действия:

1. В дереве консоли **ISA Management** щелкните правой кнопкой мыши по пункту **Protocol Definitions**, в контекстном меню последовательно выберите пункты **New** и **Definitions**.
2. В окне мастера **New Protocol Definition** укажите имя определения протокола **iBankIN** и нажмите кнопку **Next**.

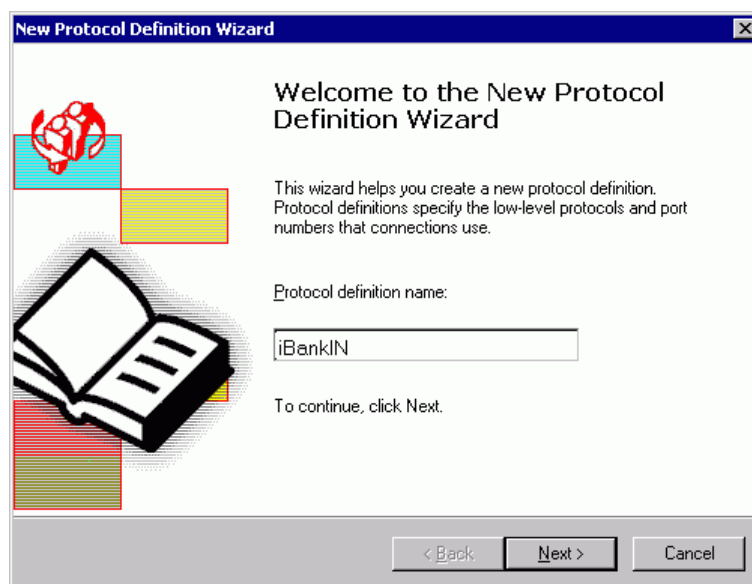


Рис. 2. Задание имени создаваемого протокола

3. На странице **Primary Connection Information** укажите порт 9091, тип протокола **HTTPS** и направление основного подключения **INCOMING**. Нажмите кнопку **Next**.
4. На странице **Secondary Connection Information** укажите, использует ли протокол дополнительные подключения. Для работы системы «iBank 2» дополнительные подключения не нужны.
5. Нажмите кнопку **Next**, а затем кнопку **Finish** для завершения работы мастера.
6. Повторите описанные выше операции и создайте протокол **iBankOUT** с направлением основного подключения **OUTGOING**.

The screenshot shows a dialog box titled "New Protocol Definition Wizard" with a close button (X) in the top right corner. The main title is "Primary Connection Information" and the instruction is "Which port number, protocol, and direction are used for the primary connection?". There is a small logo in the top right of the dialog area. The form contains three fields: "Port number:" with a text box containing "9091"; "Protocol type:" with a dropdown menu showing "TCP"; and "Direction:" with a dropdown menu showing "Outbound". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Рис. 3. Информация об основном подключении

The screenshot shows a dialog box titled "New Protocol Definition Wizard" with a close button (X) in the top right corner. The main title is "Secondary Connections" and the instruction is "Select the settings for any secondary connections.". There is a small logo in the top right of the dialog area. The form asks "Do you want to use secondary connections?" with two radio buttons: "No" (unselected) and "Yes" (selected). Below this is a table with three columns: "Port Range", "Protocol Type", and "Direction". The table is currently empty. To the right of the table are two buttons: "New..." and "Delete". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Рис. 4. Информация о дополнительных подключениях

Настройка правила протоколов

Создание правила протоколов

1. В дереве консоли **ISA Management** щелкните правой кнопкой мыши по узлу **Protocol Rules** и в контекстном меню последовательно выберите пункты **New** и **Rules**.
2. В окне мастера **New Protocol Rule** введите имя правила протоколов (iBank2) и нажмите кнопку **Next**.



Рис. 5. Задание имени правила

3. На странице **Rule Action** укажите, что данное правило разрешает подключения, выбрав пункт **Allow**, и нажмите кнопку **Next**.

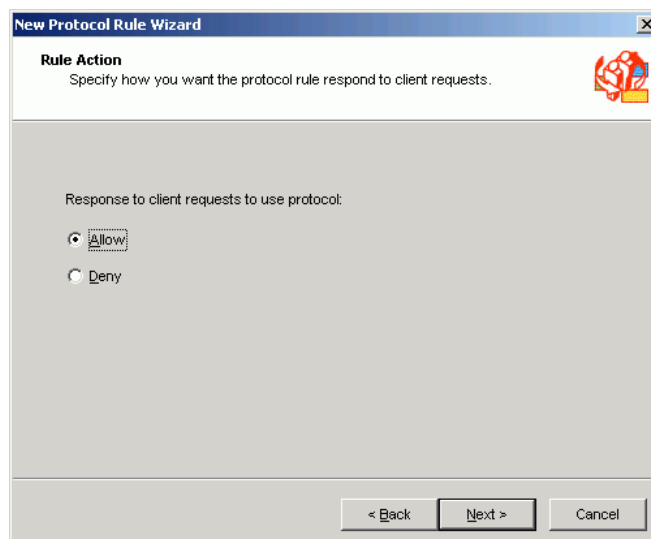


Рис. 6. Определение разрешающего правила

4. На странице **Protocols** укажите протоколы, к которым применяется данное правило (HTTPS, HTTPS Server, iBankIN, iBankOUT). Нажмите кнопку **Next**.

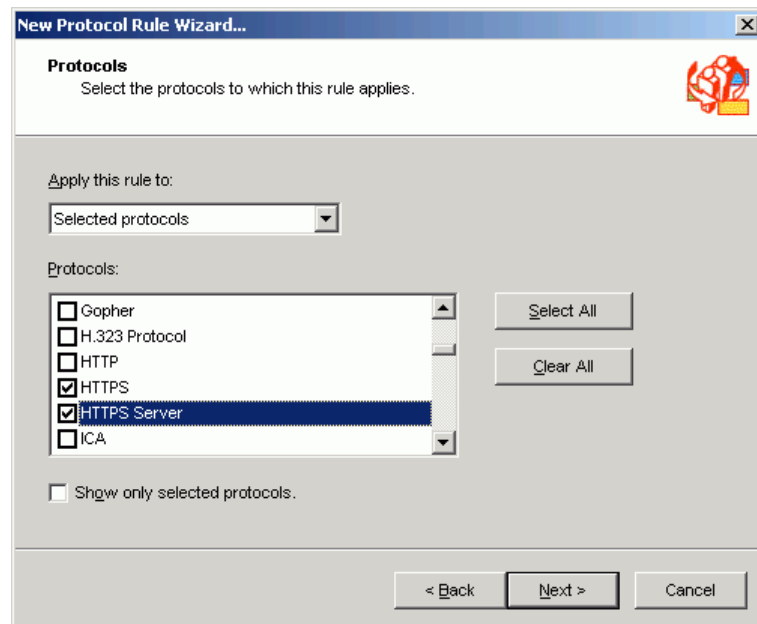


Рис. 7. Выбор протоколов правила

5. На странице **Schedule** укажите временной период, когда применяется создаваемое правило, и нажмите **Next**.

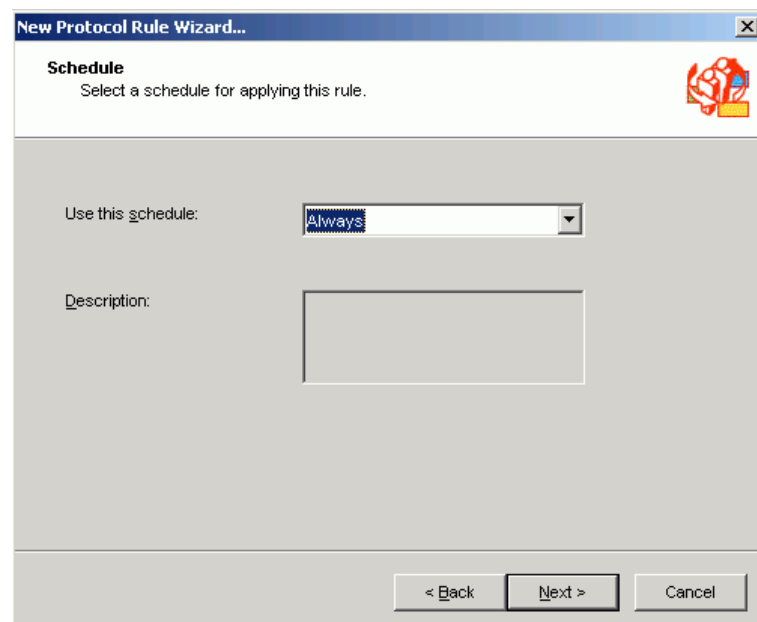


Рис. 8. Выбор расписания применения правила

6. На странице **Client Type** укажите, к каким клиентам применяется правило, и нажмите **Next**.

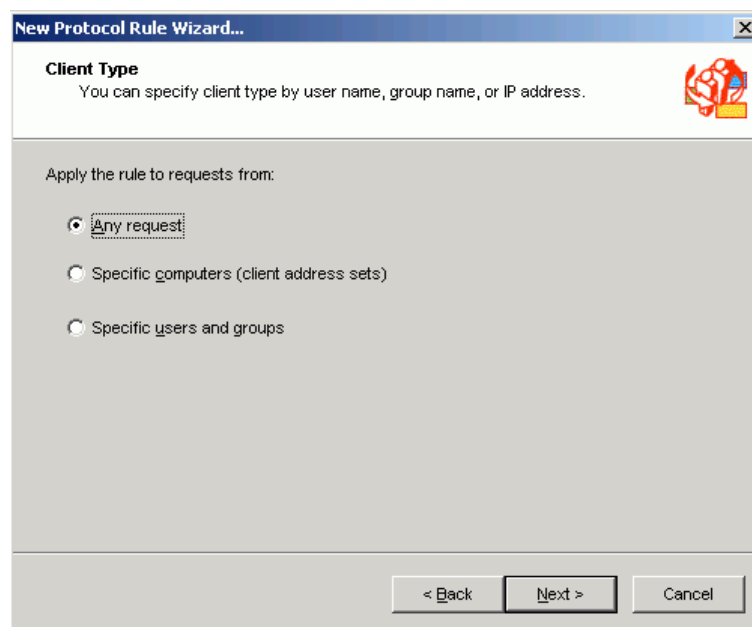


Рис. 9. Выбор клиентов, к которым применяется правило

7. В финальном окне мастера создания правила протокола нажмите **Finish**.

Если в массиве действует политика предприятия, то разрешается создавать только запрещающие правила.

Изменение правила протоколов

Администратор может изменить ранее созданные правила. Для этого откройте в дереве консоли **ISA Management** диалоговое окно свойств правил протоколов и внесите необходимые изменения, выполнив следующие действия:

1. В дереве консоли **ISA Management** выберите пункт **Protocol Rules**.
2. Откройте меню **View** и отметьте команду **Advanced**.
3. В области сведений щелкните правой кнопкой мыши по нужному правилу и в контекстном меню выберите пункт **Properties**.
4. На закладке **Protocol** выполните одно из следующих действий (см. [рис. 10](#)):
 - (a) Если правило предполагается применять ко всем протоколам, даже не определенным явно на ISA-сервере, выберите с помощью списка поля пункт **All IP Traffic** (весь IP-трафик).
 - (b) Если требуется применить правило только к выбранным протоколам, выберите с помощью списка поля пункт **Selected protocols**.
 - (c) Если требуется применить правило ко всему IP-трафику, за исключением выбранных протоколов, выберите с помощью списка поля пункт **All IP traffic except selected**.
5. В случае выбора **Selected protocols** или **All IP traffic excepted selected** отметьте в списке **Protocols** одно или несколько определений протоколов.

Если нужного определения протокола в списке нет, создайте его с помощью кнопки **New** (см. [стр. 5](#)).

Поскольку по умолчанию HTTPS запросы разрешены, обычно создание протоколов ограничивается портом 9091.

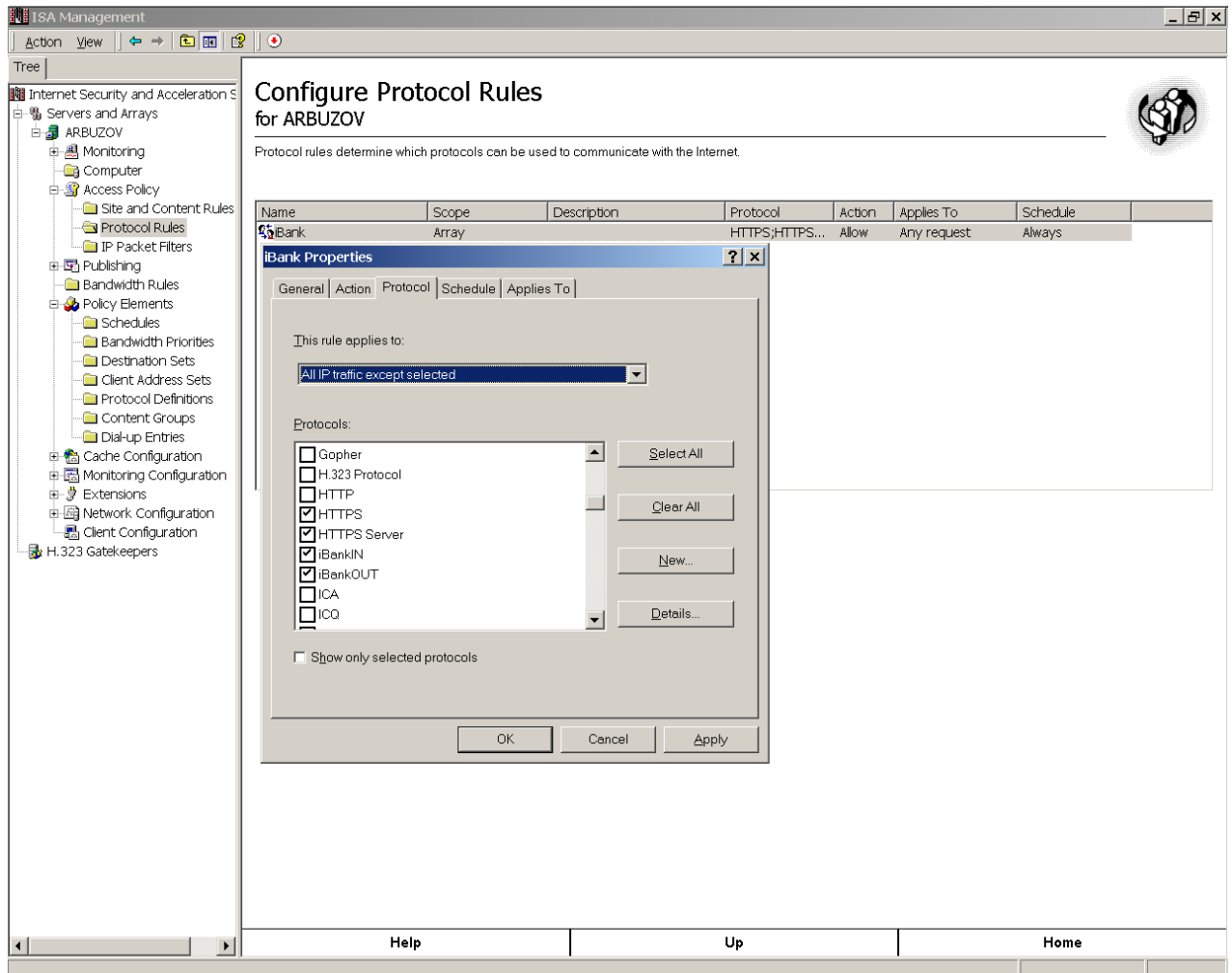


Рис. 10. Настройка правил протокола

Создание правила узлов и содержимого

1. В дереве консоли **ISA Management** щелкните правой кнопкой мыши по пункту **Site and Content Rules** и последовательно выберите пункты **New** и **Rule**.
2. В мастере создания правил узлов и содержимого **New Site and Content Rule** введите имя создаваемого правила и нажмите кнопку **Next** (см. [рис. 11](#)).



Рис. 11. Задание имени нового правила

3. На странице **Rule Action** укажите тип правила (разрешающее или запрещающее) и нажмите кнопку **Next** (см. [рис. 12](#)).

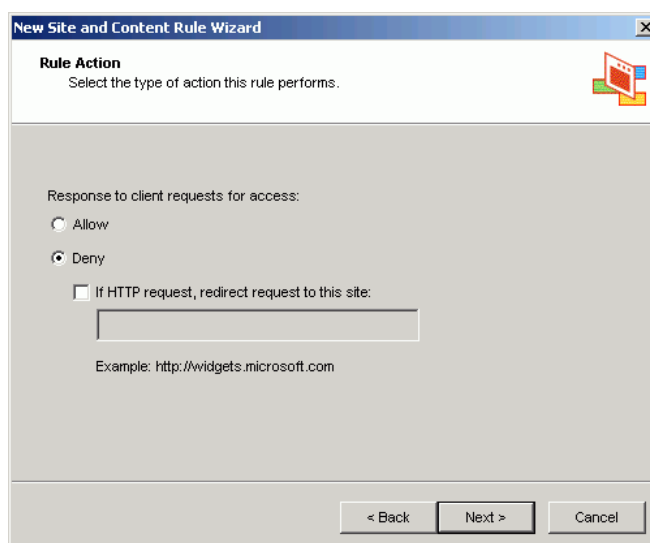


Рис. 12. Определение типа правила

4. На странице определения конфигурации правила **Rule Configuration** выберите вариант применения правила (см. [рис. 13](#)):

- к определенным узлам (**Deny access based on destination**);
- по расписанию (**Deny access only on certain times**);
- к конкретным клиентам (**Deny selected clients access to all external sites**);
- другой, пользовательский вариант (**Custom**).

Нажмите кнопку **Next**.

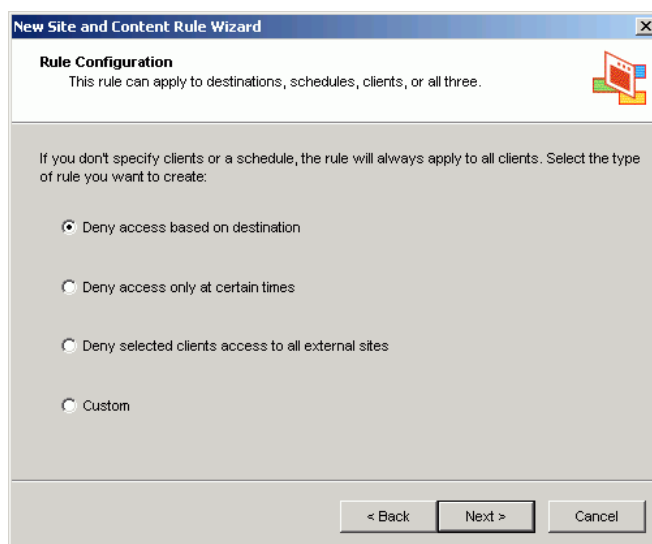


Рис. 13. Выбор варианта применения правила

Если в массиве действует политика предприятия, можно создавать только запрещающие правила.

Назначение подмножества адресатов для правила узлов и содержимого

1. В дереве консоли **ISA Management** щелкните левой кнопкой мыши по узлу **Site and Content Rules**.
2. Откройте меню **View** и отметьте команду **Advanced**.
3. В области сведений щелкните правой кнопкой мыши по нужному правилу и в контекстном меню выберите пункт **Properties**.
4. На закладке **Destinations** выберите необходимое значение с помощью списка поля **Selected destination set** (см. рис. 14).
5. В случае выбора **Selected destination set** или **All destinations except selected set** в поле **Name** укажите подмножество адресатов.

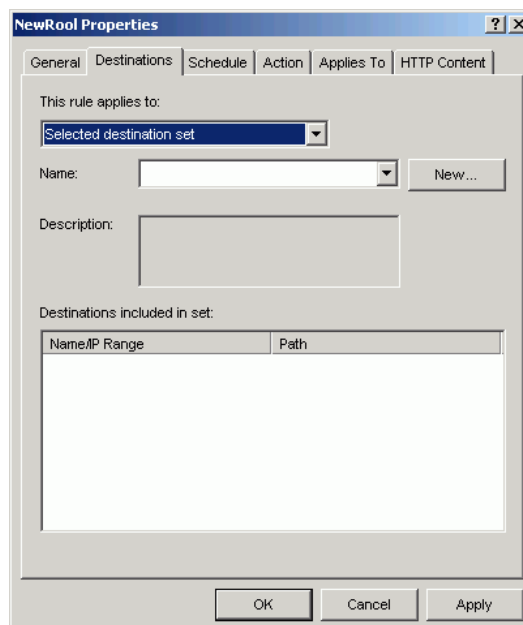


Рис. 14. Выбор адресатов для правила узлов и содержимого

Настройка фильтра IP-пакетов

Создание фильтра IP-пакетов

1. В консоли **ISA Management** щелкните правой кнопкой мыши по пункту **IP Packet Filter** и в открывшемся контекстном меню последовательно выберите пункты **New** и **Filter**. В окне мастера **New IP Packet Filter** введите имя нового фильтра и нажмите кнопку **Next** (см. рис. 15).

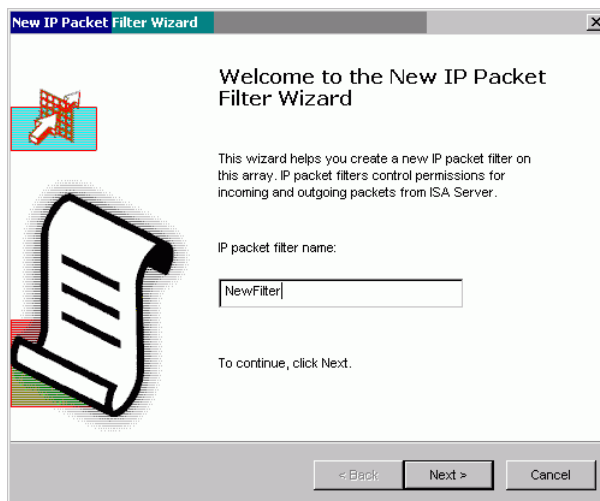


Рис. 15. Задание имени фильтра

2. На странице **Servers** укажите, нужно ли применять фильтр IP-пакетов ко всему массиву ISA-серверов или только к одному серверу.
3. На странице **Filter Mode** укажите, разрешает или блокирует фильтр прохождение пакетов (см. рис. 16).

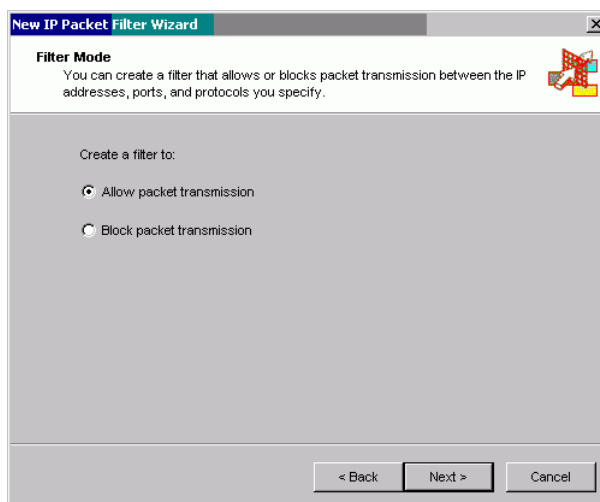


Рис. 16. Задание режима работы фильтра

4. На странице **Filter Type** выберите предустановленный тип фильтра или пункт **Custom** для создания собственного фильтра (см. [рис. 17](#)).

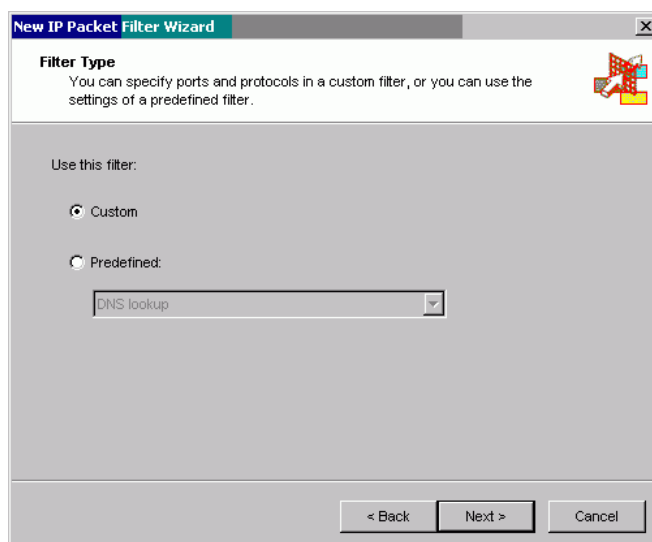


Рис. 17. Выбор типа фильтра

5. При выборе **Custom** на странице **Filter Settings** укажите IP протокол (**IP Protocol**), направление (**Direction**), локальный (**Local Port**) и удаленный (**Remote Port**) порты фильтра IP-пакетов (см. [рис. 18](#)).

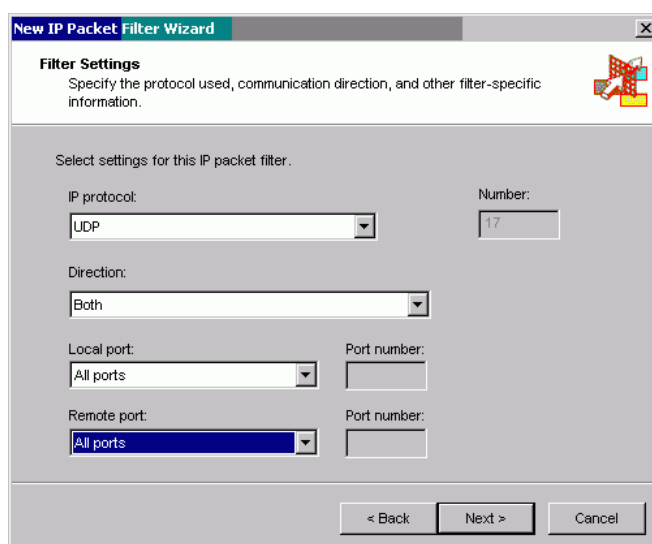


Рис. 18. Настройки фильтра

6. На странице **Local Computer** укажите локальные компьютеры, к которым будет применяться фильтр IP-пакетов (см. [рис. 19](#)).
7. На странице **Remote Computer** укажите удаленные компьютеры, к которым будет применяться фильтр IP-пакетов (см. [рис. 20](#)).

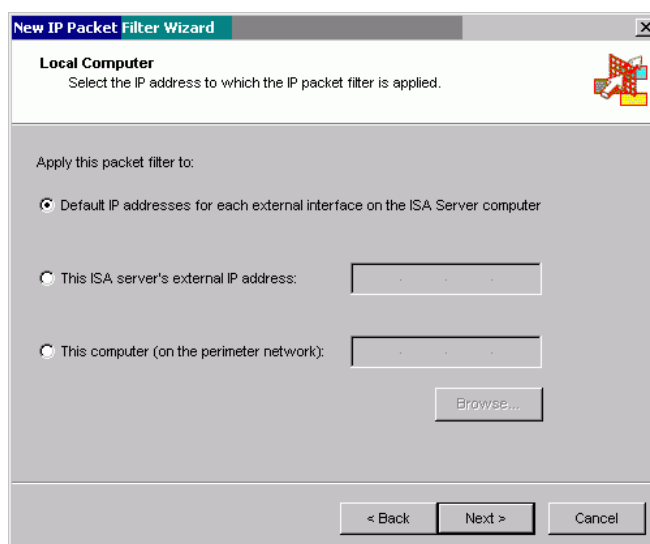


Рис. 19. Выбор локальных компьютеров

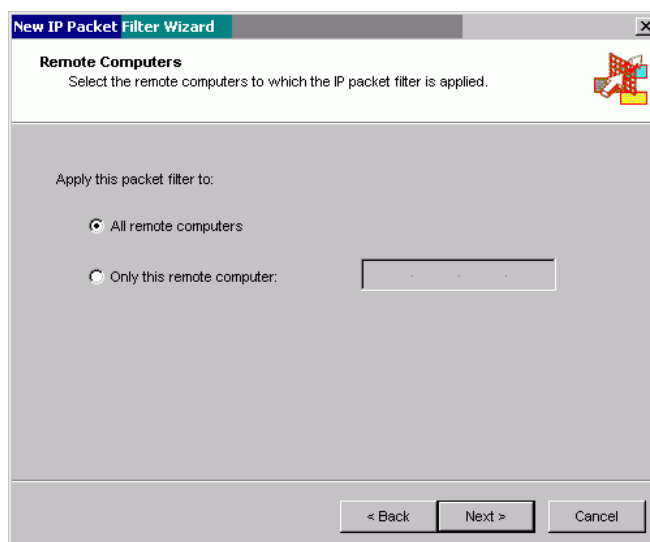


Рис. 20. Выбор удаленных компьютеров

Настройка протокола для фильтра IP-пакетов

1. Откройте меню **View** и отметьте команду **Advanced**.
2. В дереве консоли **ISA Management** выберите папку **IP Packet Filters**.
3. В области сведений щелкните правой кнопкой мыши по фильтру IP-пакетов, который требуется изменить, и в контекстном меню выберите пункт **Properties**.
4. Перейдите на закладку **Filter Type**.
5. Выполните одно из следующих действий:
 - поставьте флаг в поле **Predefined** и выберите требуемый фильтр из списка;

- проставьте флаг в поле **Custom** и с помощью списка поля **IP protocol** выберите одно из следующих значений: **Any**, **ICMP**, **TCP**, **UDP**, **Custom protocol**.
6. Если для типа фильтра **Custom** выбран произвольный протокол (пункт **Any**), с помощью списка поля **IP Protocol** укажите направление: **Inbound**, **Outbound** или **Both**.
 7. Если для типа фильтра **Custom** выбран протокол **ICMP**, выполните следующие действия:
 - С помощью списка поля **Direction** укажите одно из следующих значений: **Inbound**, **Outbound**, **Both**.
 - С помощью списка поля **Type** выберите одно из следующих значений: **All types** или **Fixed type** (для значения **Fixed type** введите **type number** в поле **Number**).
 - С помощью списка поля **Code** выберите одно из следующих значений: **All Codes** или **Fixed Code** (для значения **Fixed Code** введите **code number** в поле **Number**).
 8. Если для типа фильтра **Custom** выбран протокол **TCP**, выполните следующие действия:
 - С помощью списка поля **Direction** выберите **Inbound**, **Outbound** или **Both**.
 - С помощью списка поля **Local Port** выберите **All ports**, **Fixed port** или **Dynamic**. Для значения **Fixed port** введите номер порта в поле **Port Number**.
 - С помощью списка поля **Remote Port** выберите **All ports** или **Fixed port**. Для значения **Fixed port** введите номер порта в поле **Port Number**.
 9. Если для типа фильтра **Custom** выбран протокол **UDP**, выполните следующие действия:
 - С помощью списка поля **Direction** выберите один из следующих пунктов: **Receive only**, **Send only**, **Both**, **Receive send** или **Send receive**.
 - С помощью списка поля **Local Port** выберите **All ports**, **Fixed port** или **Dynamic**. Для значения **Fixed port** введите номер порта в поле **Port Number**.
 - С помощью списка поля **Remote Port** выберите **All ports** или **Fixed port**. Для значения **Fixed port** введите номер порта в поле **Port Number**.

Применение фильтра IP-пакетов к серверу

1. В дереве консоли **ISA Management** выберите узел **IP Packet Filters**.
2. В области сведений щелкните правой кнопкой мыши по фильтру IP-пакетов, который требуется изменить, и в контекстном меню выберите пункт **Properties** (см. [рис. 21](#)).
3. На закладке **Local computers** задайте локальный компьютер, к которому будет применяться фильтр (см. [рис. 22](#)).
4. На закладке **Remote computers** задайте удаленные компьютеры, к которым будет применяться фильтр (см. [рис. 23](#)).

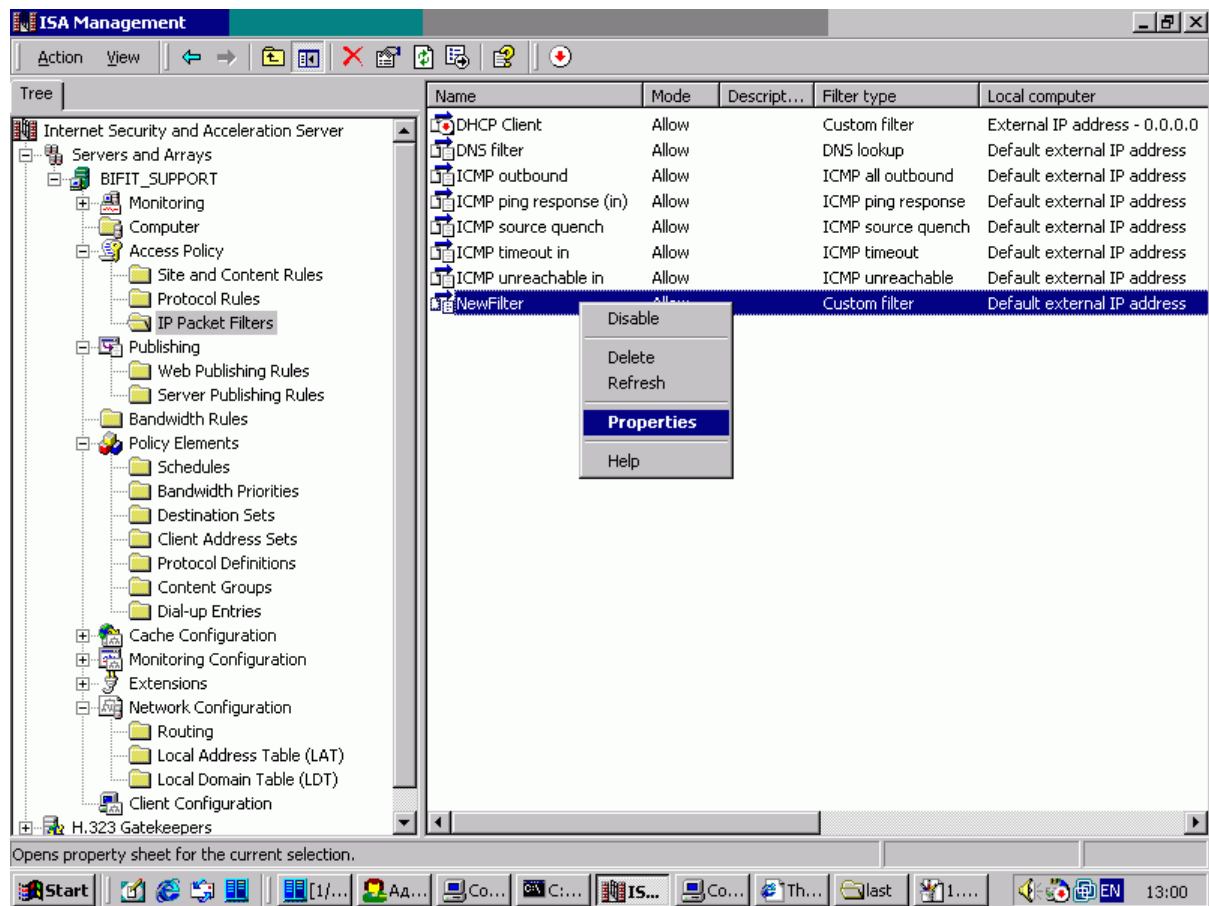


Рис. 21. Вызов окна свойств фильтра

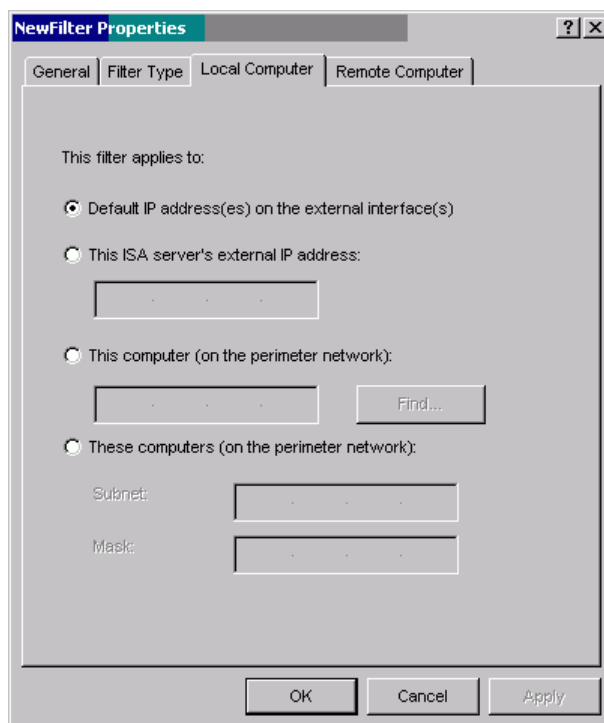


Рис. 22. Задание локального компьютера

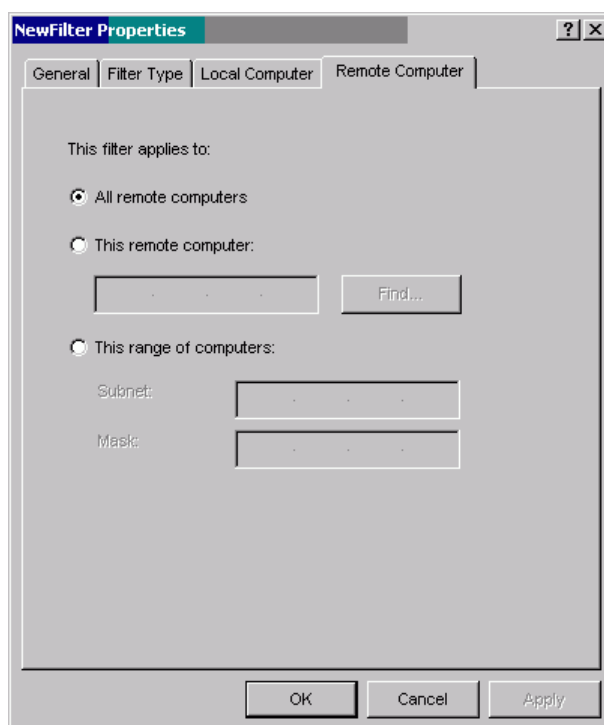


Рис. 23. Задание удаленных компьютеров