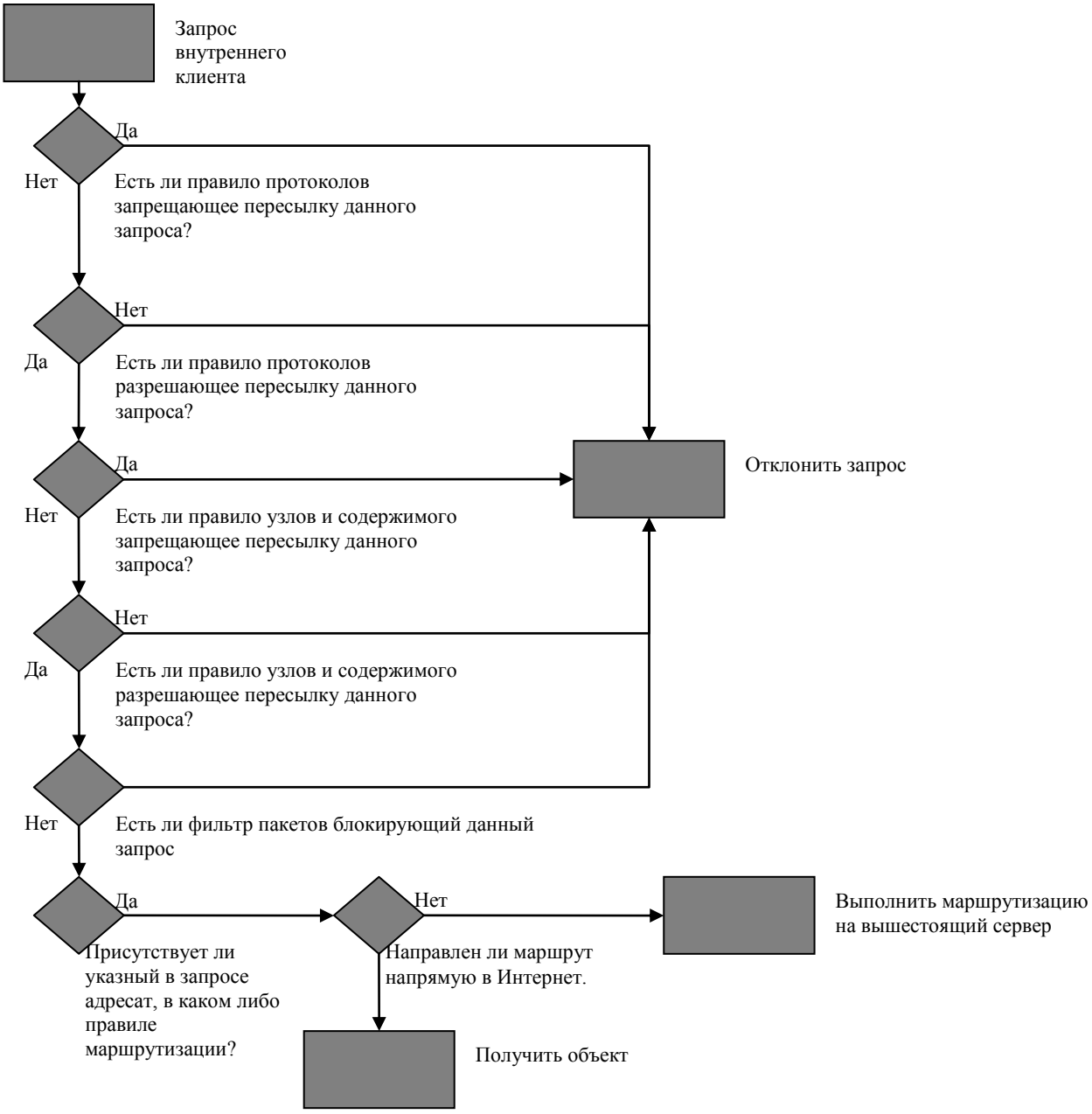
Настройка ISA сервера для работы клиента с системой iBank2

ISA сервер обрабатывает запросы следующим образом:

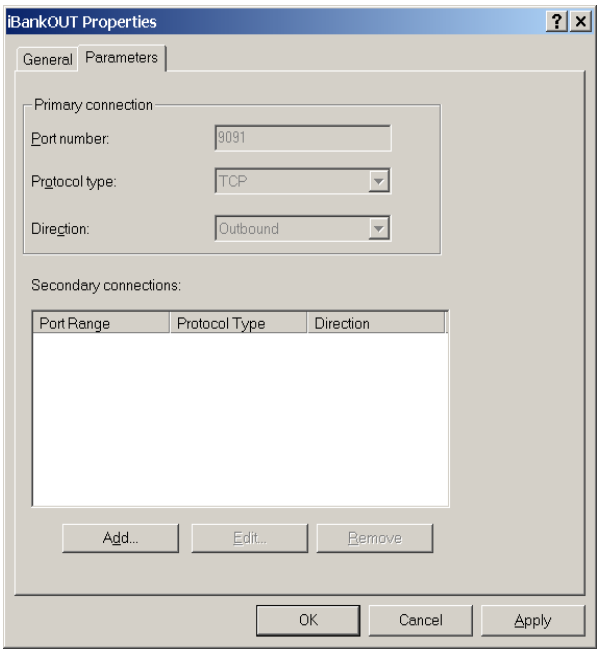


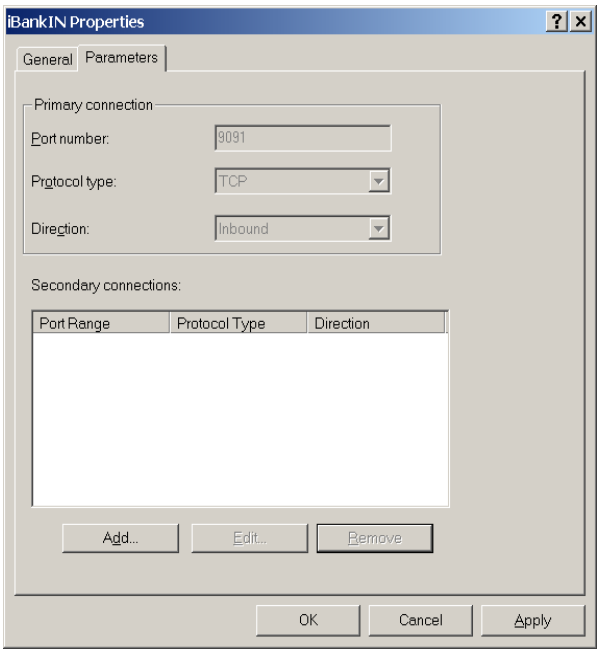
Следовательно: для работы системы необходимо выполнить следующее:

A. Отключить правила протоколов запрещающие пересылку HTTPS запросов и запросов по портам 9091
B. Создать правило протоколов разрешающее пересылку HTTPS запросов и запросов по портам 9091
C. Проверить правила узлов на наличие запрещений доступа к банку
D. Создать правило узлов разрешающее пересылку запросов
E. Проверить фильтрацию IP адресов

Создание определения протокола

I. В дереве консоли ISA Management щелкните правой кнопкой мыши узел Protocol Definitions, в контекстном меню последовательно выберите пункты New и Definition.
II. В окне мастера New Protocol Definition укажите имя определения протокола iBankIN и щелкните кнопку Next.
III. На странице Primary Connection Information укажите порт 9091, тип протокола HTTPS и направление основного подключения INCOMING и щелкните кнопку Next.
IV. На странице Secondary Connections нужно указать, использует ли протокол дополнительные подключения. Для работы системы iBank дополнительные подключения не нужны.
V. Щелкните кнопку Next, а затем кнопку Finish, чтобы завершить работу с мастером
VI. Повторить процедуры и создать протокол iBankOUT с направлением подключения OUTGOING





Создание правила протоколов

I. В дереве консоли ISA Management щелкните правой кнопкой мыши узел Protocol Rules и в контекстном меню последовательно выберите пункты New и Rule.
II. В окне мастера New Protocol Rule введите имя правила протоколов (BIFIT) , затем щелкните кнопку Next.
III. На странице Rule Action укажите что данное правило разрешает подключения Allow, и щелкните кнопку Next.
IV. На странице Protocols укажите протоколы, к которым применяется правило(HTTPS, HTTPS Server, iBankIN, iBankOUT), и щелкните кнопку Next.
V. На странице Schedule укажите, когда применяется правило, и щелкните кнопку Next.
VI. На странице Client Type укажите, к каким клиентам применяется правило, и щелкните кнопку Next.

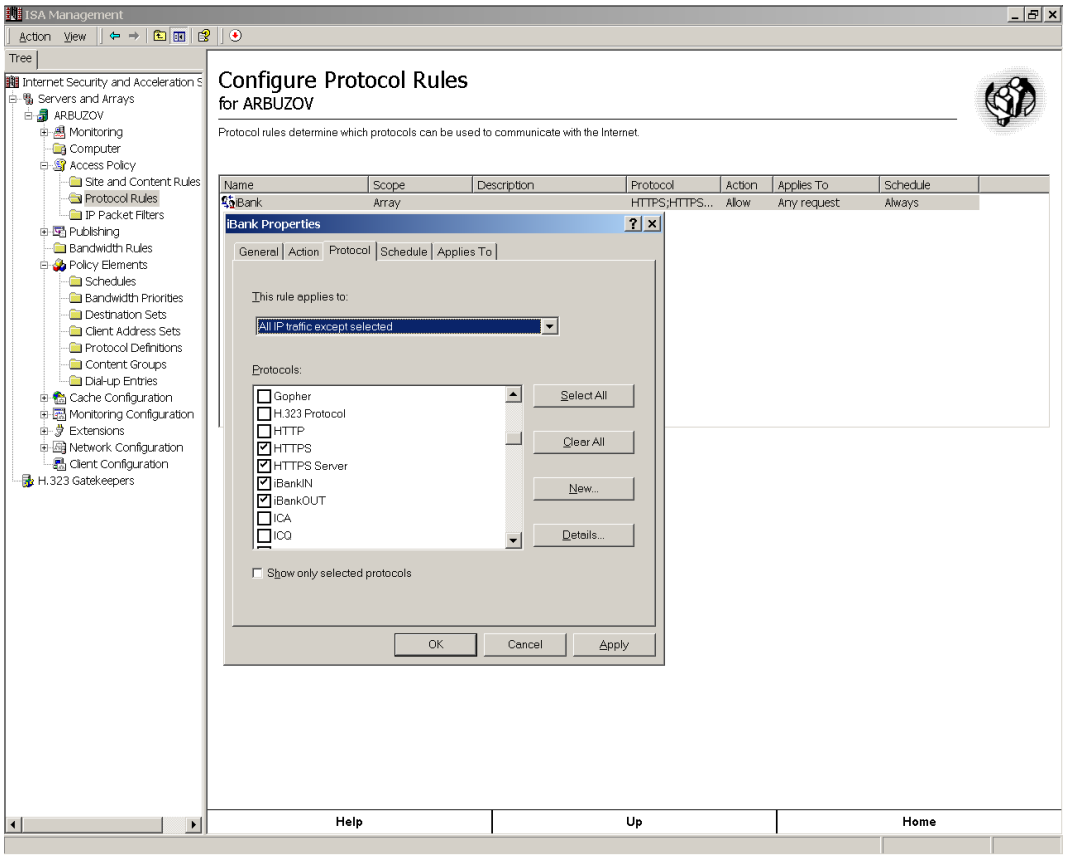
Примечание: Если в массиве действует политика предприятия, разрешается создавать только запрещающие правила.

Администратор может в любой момент внести изменения в ранее созданные правила. Для этого достаточно открыть в консоли ISA Management диалоговое окно свойств правила протоколов и выполнить нужные операции.

Изменение правила протоколов

I. В дереве консоли ISA Management выберите узел Protocol Rules.
II. Откройте меню View и отметьте команду Advanced.
III. В области сведений щелкните правой кнопкой мыши нужное правило и в контекстном меню укажите Properties.
IV. На вкладке Protocol выполните одно из следующих действий:
    a. если правило предполагается применять ко всем протоколам, даже не определенным явно на ISA-сервере, выберите в поле со списком All IP Traffic (весь IP-трафик);
    b. если требуется применить правило только к выбранным протоколам, укажите в поле со списком Selected protocols;
    c. если требуется применить правило ко всему IP-трафику, за исключением выбранных протоколов, щелкните в поле со списком All IP traffic except selected.
V. В случае выбора Selected protocols или All IP traffic excepted selected отметьте в списке Protocols одно или несколько определений протоколов.
   Примечание: Если нужного определения протокола в списке нет, создайте его, щелкнув кнопку New.

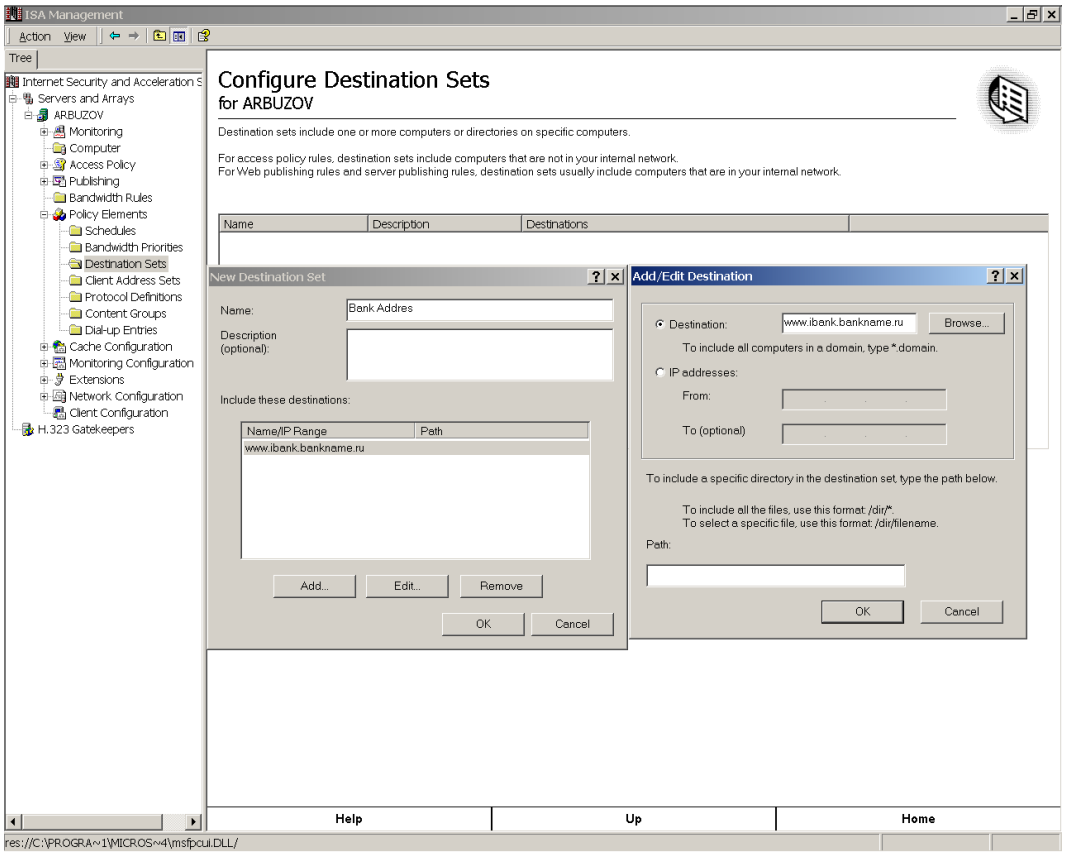
Примечание: Обычно по умолчанию HTTPS запросы разрешены. Необходимо создать протоколы по порту по порту 9091



Создание правила узлов и содержимого:

I. В дереве консоли ISA Management щелкните правой кнопкой мыши узел Site and Content Rules и последовательно выберите в контекстном меню пункты New и Rule.
II. В мастере создания правила узлов и содержимого New Site and Content Rule введите имя правила и щелкните кнопку Next.
III. На странице Rule Action укажите тип правила — разрешающее или запрещающее — и щелкните кнопку Next.
IV. На странице определения конфигурации правила Rule Configuration выберите вариант применения правила: 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) или другой, пользовательский вариант (Custom). Щелкните кнопку Next.

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



Назначение подмножества адресатов для правила узлов и содержимого

I. В дереве консоли ISA Management щелкните узел Site and Content Rules.
II. Откройте меню View и отметьте команду Advanced.
III. В области сведений щелкните правой кнопкой мыши нужное правило и в контекстном меню выберите Properties.
IV. На вкладке Destinations выберите одно из значений в поле со списком Selected destination set;
V. В случае выбора Selected destination set или All destinations except selected set в поле Name укажите подмножество адресатов.

Создание фильтра IP-пакетов

I. В консоли **ISA Management** щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню последовательно выберите пункты **New** и **Filter.**
II. В окне мастера **New IP Packet Filter** введите имя нового фильтра и щелкните кнопку Next.
III. На странице **Servers** укажите, нужно ли применять фильтр IP-пакетов ко всему массиву ISA-серверов или только к одному из серверов.
IV. На странице **Filter Mode** укажите, разрешает или блокирует фильтр прохождение пакетов.
V. На странице **Filter Type** выберите предустановленный фильтр или переместите переключатель в положение Custom, чтобы создать новый тип фильтра.
VI. В случае выбора Custom на странице **Filter Settings** укажите IP-протокол (**IP protocol**), направление (**Direction**), локальный (**Local port)** и удаленный (**Remote port**) порты фильтра IP-пакетов.
VII. На странице **Local Computer** укажите компьютер локальной сети, к которому будет применяться фильтр IP-пакетов.
VIII. На странице **Remote Computers** укажите удаленные компьютеры, к которым будет применяться фильтр IP-пакетов.

Примечание: Чтобы внесенные изменения вступили в силу после создания фильтра или изменения конфигурации фильтра IP-пакетов, необходимо перезапустить службы ISA-сервера.

Настройка протокола для фильтра IP-пакетов

I. Откройте меню **View** и отметьте команду **Advanced**.
II. В дереве консоли ISA Management щелкните папку **IP Packet Filters**.
III. В области сведений щелкните правой кнопкой мыши фильтр IP-пакетов, который требуется изменить, и в контекстном меню выберите команду **Properties.**
IV. Перейдите на вкладку **Filter Type.**
V. Выполните одно из следующих действий:
• установите переключатель в положение **Predefined** и выберите фильтр из списка;
• установите переключатель в положение Custom и в поле со списком IP protocol выберите одно из значений: **Any, ICMP, TCP, UDP** или **Custom protocol.**
VI. Если выбран переключатель **Custom** и протокол **ICMP**, выполните следующие действия:
• в поле со списком **Direction** укажите одно из значений: **Inbound, Outbound** или **Both**;
• в поле со списком Type выберите одно из значений: **All types** или **Fixed Type**. Если вы выбрали **Fixed type**, введите **type number** в поле **Number**;
• в поле со списком **Code** щелкните **All Codes** или **Fixed Code**. Если вы указали **Fixed Code**, введите code number в поле **Number.**
VII. Если выбраны переключатель Custom и элемент Any, в списке IP Protocol укажите направление: Inbound, Outbound или Both.
VIII. Если выбран переключатель Custom и протокол UDP, выполните следующие действия:
• в поле со списком Direction щелкните Receive only, Send only, Both, Receive send или Send receive;
• в поле со списком Local Port укажите All ports, Fixed port или Dynamic. Если выбран Fixed port, укажите номер порта в поле Port number;
в поле со списком Remote port щелкните All ports или Fixed port. Если выбран Fixed port, введите порт в поле Port number.
IX. Если выбран Custom и протокол TCP, выполните следующие действия:
• в поле со списком Direction щелкните Inbound, Outbound или Both;
• в поле со списком Local port укажите All ports, Fixed port или Dynamic. Если выбран Fixed port, введите номер порта в поле Port Number;
• в поле со списком Remote Port выберите All Ports или Fixed Port. Если выбран Fixed port, укажите номер порта в поле Port number.

Применение фильтра IP-пакетов к серверу
Откройте меню View и отметьте команду Advanced.

I. В дереве консоли ISA Management щелкните узел IP Packet Filters.
II. В области сведений щелкните правой кнопкой мыши фильтр IP-пакетов, который требуется изменить, и в контекстном меню выберите команду Properties.
III. На вкладке General в разделе Servers that use this filter (серверы, использующие этот фильтр) выполните одно из следующих действий:
• установите переключатель в положение All servers in the array (все серверы массива);
• установите переключатель в положение Only this server (только этот сервер) и затем выберите сервер, к которому будет применяться фильтр.