Работа клиента через Firewall. Рекомендации

В общем случае возможны два варианта работы клиента с Интернет – непосредственное подключение и работа через Firewall (Firewall - межсетевой экран, в рамках которого реализуется политика Интернет-безопасности).

Первый вариант – непосредственное подключение – предполагает, что клиент непосредственно подключен к Интернет, и его рабочий компьютер имеет реальный IP-адрес. В подавляющем большинстве случаев именно такое соединение получает клиент, когда подключается к Интернет по Dialup. Когда же клиент имеет выделенный канал к себе в офис, подключение, как правило, осуществляется через Firewall.

В случае непосредственного соединения никаких особенностей при работе клиента в системе «iBank» не возникает. Java-апплеты непосредственно взаимодействуют с Сервером «iBank».

Особенности могут возникать (и как правило возникают) при подключении клиента к Интернет через Firewall.

В общем случае Firewall может выполнять следующие функции:

- ✓ IP-фильтрация
- ✓ трансляция IP-адресов
- ✓ прокси-сервер

Рассмотрим особенности работы клиента при использовании на Firewall’е каждой из этих трех функций.

IP-фильтрация (IP-filter). Firewall осуществляет фильтрацию трафика в соответствии с правилами, заданными администратором. Практически всегда реализуется политика «Все что явно не разрешено – запрещено». Соответственно в правилах фильтрации для работы Java-апплетов на Firewall’е необходимо открыть следующие TCP-порты:

- ✓ TCP-порт 443 – для соединения Web-браузера клиента с Web-сервером банка по протоколу SSL
- ✓ TCP-порт 33333 – для работы Java-апплета «Рублевые документы» с Сервером «iBank»
- ✓ TCP-порт 33334 – для работы Java-апплета «Регистратор» с Сервером «iBank»
- ✓ TCP-порт 33335 – для работы Java-апплета «Валютные документы» с Сервером «iBank»

В общем случае банк может изменить TCP-порты 33333..33335 на любые другие. В этом случае, необходимо связаться с администратором банка и уточнить номера портов, которые необходимо открыть в IP-фильтре на Firewall’е.

Трансляция IP-адресов (NAT – Network Address Translation). Firewall осуществлять подмену реальных IP-адресов на fake IP-адреса из специально зарезервированных для этих целей подсетей (например из подсетки 192.168.0.0). В этом случае сетевому интерфейсу на компьютере клиента назначен fake IP-адрес. Данная функция Firewall’а никак не влияет на работоспособность Web-браузера и Java-апплетов, и клиент прекрасно и без проблем может работать с системой «iBank».

Прокси-сервер (Proxy Server). Прокси-серверов существует достаточно много. Далее рассмотрим наиболее часто используемое ПО.

Squid. Рекомендации по настройке

Процесс установки и первоначальной настройки прокси-сервера Squid здесь не рассматривается. Далее приведены только рекомендации, следование которым необходимо для успешной работы клиентов с Сервером «iBank», установленным в банке.

Для обеспечения работы Java-апплетов с Сервером «iBank» через прокси-сервер Squid необходимо соблюдение следующих правил:

1. Не должна использоваться аутентификация клиентов - Squid не должен запрашивать у пользователя его имя и пароль. Соответственно не следует использовать директиву

   ```
   acl <acl_name> proxy_auth REQUIRED
   ```

   в файле настроек `squid.conf`.

   Если же существует необходимость в использовании этого механизма защиты, то необходимо отключить аутентификацию клиентов при обращении к серверу iBank. Для этого нужно добавить в `squid.conf` следующие строчки:

   ```
   acl ibank_dst dst 195.239.34.170/255.255.255.255 (ip адрес сервера iBank)
   acl ibank_ports port 443 33333-33335
   http_access allow ibank_dst
   http_access allow CONNECT ibank_ports
   ```

   Примечание. Последние две строчки должны быть записаны до строки, в которой запрашивается аутентификация, т.е. если существует access-лист, допустим, `users` в виде

   ```
   acl users proxy_auth REQUIRED
   ```

   то наши две строки должны располагаться до строки

   ```
   http_access allow users
   ```

2. Разрешить соединения на TCP-порты 443, 33333-33335 Сервера «iBank». Возможный вариант:

   ```
   acl ibank_ports port 443 33333-33335
   http_access allow CONNECT ibank_ports
   ```

   Причем последняя строчка должна располагаться до строки, в которой вводится запрет на порты выше 1023. В стандартной поставке Squid разрешены порты: 80, 21, 443, 563, 70, 210, 1025-65535. Многие оставляют только 80, 443, поэтому здесь нужно быть внимательным.

3. При запуске апплетов системы iBank пользователю нужно указывать ip адрес и порт (3128 по умолчанию) proxy-сервера Squid.

Microsoft Proxy Server. Рекомендации по настройке

Процесс установки и первоначальной настройки Microsoft Proxy Server здесь не рассматривается. Далее приведены только рекомендации, следование которым необходимо для успешной работы клиентов с Сервером «iBank», установленным в банке.

Для обеспечения работы Java-апплетов с Сервером «iBank» через Microsoft Proxy Server необходимо клиенту установить и настроить пакет Microsoft Proxy Client. В результате у клиента будет установлена новая версия WinSock, обеспечивающая прозрачную работу сетевых приложений клиента через Microsoft Proxy Server.

Из сервисов Microsoft Proxy Server для работы клиента достаточно только сервиса WinSock Proxy. При этом в настройках Web-браузера клиента и при запуске Java-апплетов **не нужно** указывать IP-адрес и TCP-порт используемого прокси-сервера.

Microsoft Internet Security & Acceleration Server (ISA Server)

Рекомендации по настройке

Процесс установки и первоначальной настройки ISA Server здесь не рассматривается. Далее приведены только рекомендации, следование которым необходимо для успешной работы клиентов с Сервером «iBank», установленным в банке.

Настройка ISA Server осуществляется в ISA Management.

При соединении через ISA Server не должна использоваться аутентификация клиентов - ISA Server не должен запрашивать у пользователя его имя и пароль. Чтобы проверить это, необходимо раскрыть дерево

Internet Security and Acceleration Server
Servers and Arrays
Server_Name

В *Properties* в закладке *Outgoing Web Requesters* галочки *«Ask unauthenticated users for identification»* быть не должно.

Необходимо разрешить соединение по протоколу SSL с Сервером «iBank». Для этого необходимо раскрыть дерево

Internet Security and Acceleration Server
Servers and Arrays
Server_Name
Access Policy
Protocol Rules

и создать новое правило, при этом:

- На шаге *Rule Action* указать *Allow.*
- На шаге *Protocols* выбрать *Selected protocols.* В списке протоколов напротив HTTPS поставить галочку.
- На шаге *Schedule* выбрать *Always.*
- На шаге Client Type выбрать *Specific computers (clients address set).*
- На шаге *Client Set* указать IP-адреса компьютеров, на которых исполняются Java-апплеты системы «iBank».

В системе «iBank» взаимодействие Java-апплетов с Сервером Приложения осуществляется по криптопротоколу GSL (аналогичен протоколу SSL, но содержит российские криптоалгоритмы). ISA Server распознаёт этот GSL как протокол SSL. Однако, по умолчанию, ISA Server поддерживает работу по протоколу SSL только через порты 433 и 653. Для того, чтобы обеспечить работу по SSL (и GSL) через другие порты, необходимо выполнить следующие действия:

1. Создать на сервере ISA файл с расширением '.vbs' (VBScript) и следующим содержанием:

```
set isa=CreateObject("FPC.Root")
set tprange=isa.Arrays.GetContainingArray.ArrayPolicy.WebProxy.TunnelPortRanges
set tmp=tprange.AddRange("Rubles 1.8 : 33333", 33333, 33333)
tprange.Save
set isa=CreateObject("FPC.Root")
set tprange=isa.Arrays.GetContainingArray.ArrayPolicy.WebProxy.TunnelPortRanges
set tmp=tprange.AddRange("Currency 1.8 : 33335", 33335, 33335)
tprange.Save
set isa=CreateObject("FPC.Root")
set tprange=isa.Arrays.GetContainingArray.ArrayPolicy.WebProxy.TunnelPortRanges
set tmp=tprange.AddRange("Registrator 1.8 : 33334", 33334, 33334)
tprange.Save
```

2. Двойным щелчком левой кнопки мыши запустить его на исполнение.

3. Рестартовать сервисы Web-proxy и Firewall (используя ISA Management).