Работа клиента через Firewall. Рекомендации

Версия 1.0

Оглавление

Введение

Данное руководство предназначено для клиентов банка. Документ предоставляет общую информацию о Firewall, а также о настройках наиболее часто используемых прокси-серверов для работы с системой электронного банкинга iBank 2 UA.

Глава **Общая информация о Firewall** предоставляет сведения о межсетевом экране. Рассматриваются возможные пути подключения клиента к Интернет, а также функции, выполняемые Firewall.

Инструкции по настройке наиболее широко распространенных прокси-серверов Squid, Microsoft Proxy Server и Microsoft Internet Security and Acceleration Server для работы с системой iBank 2 UA приведены в главе **Настройка прокси-сервера**.

Глава 1

Общая информация о Firewall

В общем случае возможны два варианта работы клиента с Интернет:

1. **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 Dial-up.
2. **Работа через Firewall**. Firewall — это межсетевой экран, в рамках которого реализуется политика Интернет-безопасности. Firewall используется, как правило, при подключении клиента к Интернет через выделенный канал.

В случае непосредственного соединения никаких особенностей при работе клиента в системе iBank 2 UA не возникает. Java-апплеты непосредственно взаимодействуют с Сервером Приложений.

Особенности могут возникать при подключении клиента к Интернет через Firewall. В общем случае Firewall может выполнять следующие функции:

- IP-фильтрация (IP-filter);
- Трансляция IP-адресов (NAT - Network Address Translation);
- Прокси-сервер (Proxy Server).

Особенности работы клиента при использовании каждой из этих трех функций на Firewall рассматриваются далее в главе.

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 необходимо открыть:

- TCP-порт 443 — для соединения Web-браузера клиента с Web-сервером банка по протоколу SSL;

Также необходимо связаться с администратором банка и уточнить номера портов, которые необходимы для подключения клиентских апплетов, после чего открыть эти порты.

Трансляция IP-адресов (NAT - Network Address Translation)

Firewall осуществляет 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 никак не влияет на работоспособность Web-браузера и Java-апплетов, и клиент может успешно работать с системой iBank 2 UA.

Прокси-сервер (Proxy Server)

Прокси-сервер — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Прокси-серверов существует достаточно много. В следующей главе будет рассмотрено наиболее часто используемое ПО.

Глава 2

Настройка прокси-сервера

Процесс установки и первоначальной настройки прокси-серверов в данном документе не рассматривается. Ниже приведены рекомендации, следование которым необходимо для успешной работы клиентов с Сервером Приложений iBank 2 UA, установленным в банке.

Squid

В данном разделе будет применятся такое обозначение: `%ports%` — перечень открытых портов[1], указанных в настройках Firewall (см. подраздел IP-фильтрация (IP-filter)).

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

1. Не должна использоваться аутентификация клиентов — Squid не должен запрашивать у пользователя его имя и пароль. Для этого не следует в файле настроек `squid.conf` использовать директиву:

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

   Если же существует необходимость в использовании этого механизма защиты, то следует отключить аутентификацию клиентов при обращении к Серверу Приложений. 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 2 UA)
   acl ibank_ports port %ports%
   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, например, `users` в виде `acl users proxy_auth REQUIRED` то вышеупомянутые две строки должны располагаться до строки `http_access allow users`.

2. Разрешить соединения на открытые TCP-порты Сервера Приложений. Возможный вариант:

   ```
   acl ibank_ports port %ports%
   http_access allow CONNECT ibank_ports
   ```

[1] В программном коде порты перечисляются без запятой

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.

3. При запуске апплетов системы iBank 2 UA пользователю нужно указывать IP-адрес и порт (3128 по умолчанию) proxy-сервера Squid.

Microsoft Proxy Server

Для обеспечения работы Java-апплетов с Сервером Приложений через Microsoft Proxy Server клиенту необходимо 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 and Acceleration Server

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** снять метку **Ask unauthenticated users for identification**.

Необходимо разрешить соединение по протоколу SSL с Сервером Приложений. 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 отметить меткой **HTTPS**;
- 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 функционируют Java-апплеты системы iBank 2 UA.

В системе iBank 2 UA взаимодействие Java-апплетов с Сервером Приложений осуществляется по криптопротоколу GSL (аналогичен протоколу SSL, но содержит украинские 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 : 9091", 9091, 9091)
   tprange.Save
   ```

   Список портов необходимо уточнить у банковского администратора.

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

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