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 «АСЭД» не возникает. Java-апплеты непосредственно взаимодействуют с Сервером «АСЭД».

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 9091 – для работы Java-апплета «Рублевые документы» с Сервером «АСЭД»
- ✓ TCP-порт 9091 – для работы Java-апплета «Регистратор» с Сервером «АСЭД»
- ✓ TCP-порт 9092 – для работы Java-апплетов с Сервером «АСЭД» в некоторых случаях

В общем случае банк может изменить TCP-порты 9091..9092 на любые другие. В этом случае, необходимо связаться с сетевым администратором банка (admin@deal-bank.ru) 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 «АСЭД».

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 «АСЭД», установленным в банке.

Для обеспечения работы Java-апплетов с Сервером «АСЭД» 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 «АСЭД». Для этого нужно добавить в `squid.conf` следующие строчки:

   ```
   acl ased_dst dst 213.189.201.177/255.255.255.255 (ip адрес сервера «АСЭД»)
   acl ased_ports port 443 9091-9092
   http_access allow ased_dst
   http_access allow CONNECT ased_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, 9091-9092 и др. Сервера «АСЭД». Возможный вариант:

   ```
   acl ased_ports port 443 9091-9092
   http_access allow CONNECT ased_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 «АСЭД» 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 «АСЭД», установленным в банке.

Для обеспечения работы Java-апплетов с Сервером «АСЭД» 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.