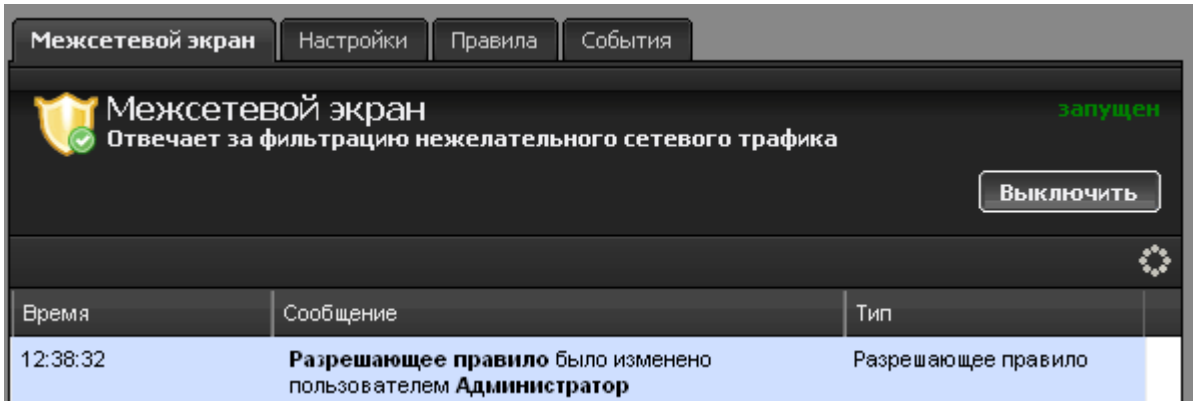
Межсетевой экран

Стартовая страница модуля

Межсетевой экран — комплекс программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также, межсетевой экран ИКС отвечает за трансляцию сетевых адресов во внешнюю сеть (NAT) и перенаправление портов.



При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние события системы.

Внимание! Выключение межсетевого экрана оставит работающими только правила NAT'а. Все правила, ограничивающие доступ извне, будут отключены, что может негативно сказаться на безопасности системы. Отключайте межсетевой экран только при крайней необходимости.

Также следует отметить, что после перезагрузки системы с выключенным межсетевым экраном список правил pf, в том числе и правила NAT'а будет полностью очищен, и пользователи потеряю доступ во внешнюю сеть по всем протоколам, кроме HTTP.

Настройки

Вкладка «Настройки» позволяет определить уровень доступа к управлению ИКС без создания дополнительных правил межсетевого экрана. Вы можете прописать ip-адреса или подсети, с которых будет осуществляться доступ к веб-интерфейсу ИКС или к консоли восстановления по протоколу SSH.

Если вы хотите получать доступ к ИКС из любого места, вы можете полностью открыть доступ, прописав подсеть 0.0.0.0/0. **Внимание! Данная настройка не является безопасной, поскольку в таком случае любой может получить доступ к системе.** Перед тем, как открывать доступ, настоятельно рекомендуется изменить пароль открываемого сервиса на

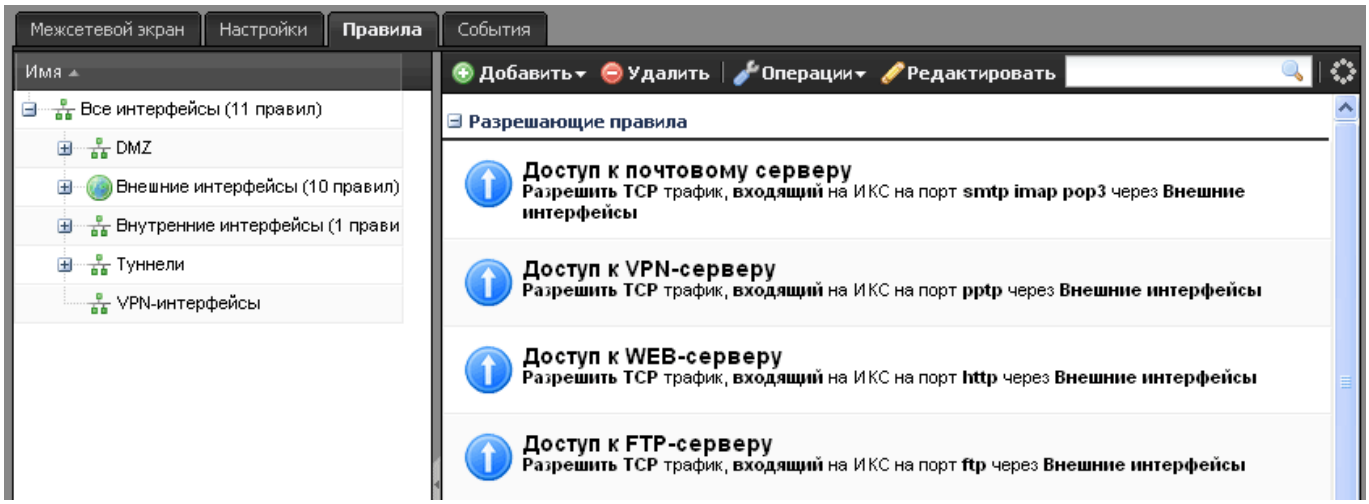
более безопасный (не менее восьми символов, включающих цифры и буквы различного регистра).

Параметр «Максимальное количество активных соединений» позволяет установить лимит всех сетевых подключений к системе.

Параметр «Режим работы межсетевого экрана» устанавливает очередность запуска модулей pf и ipfw. В некоторых случаях работа VPN-подключений через ИКС может быть затруднена прохождением через NAT модуля pf. В таком случае измените очередность запуска на pf→ipfw.

Правила

Вкладка «Правила» является главным рабочим полем администратора по настройке межсетевого экрана. Она разделена на две части: список всех интерфейсов ИКС (в виде дерева) и собственно списка правил. При клике на выбранном интерфейсе будут показаны только те правила, которые относятся к данному интерфейсу. При необходимости вы можете отключить список интерфейсов, нажав на значок в виде стрелки в центре разделительной полосы.



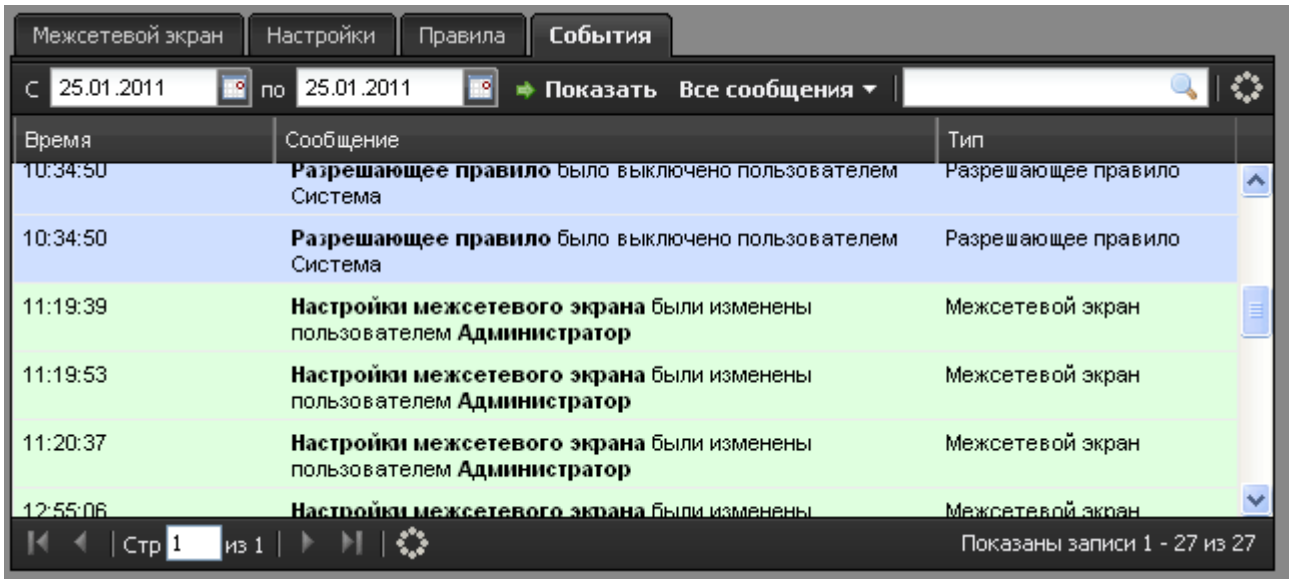
Правила межсетевого экрана группируются по типу:

1. Разрешающие правила
2. Запрещающие правила
3. Приоритеты
4. Маршруты
5. Ограничения скорости

По умолчанию в межсетевом экране все соединения, инициированные снаружи, запрещены. При установке создаются несколько стандартных разрешающих правил для корректной работы основных сервисов: почтовый сервер (порты 25, 110, 143), FTP-сервер (порты 21, 10000-10030), веб-сервер (порт 80), DNS-сервер (порт 53 UDP), VPN-сервер (порт 1723, протокол GRE). Также создаются два отключенных разрешающих правила: доступ к samba-ресурсам (порты 139, 445) и доступ к трансферу зон DNS (порт 53 TCP) и правило, разрешающее отвечать на ICMP-запросы (пинги). Эти правила не являются жестко заданными, при необходимости вы можете их выключить, отредактировать или удалить.

События

Вкладка «События» отображает все изменения, происходящие с межсетевым экраном. Она разделена на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать нужные вам записи.



Вкладка всегда отображает события за текущую дату. Чтобы посмотреть события за другой день или иной промежуток времени, выберите нужные даты, используя календарь в левом верхнем углу модуля.

В правой части верхней панели выпадающее меню «Сообщения» позволяет отфильтровать список событий по выбранному критерию: системные сообщения, сервисные сообщения, ошибки, остальные сообщения.