Универсальное программное обеспечение для сетевых устройств NETSHe.

Руководство пользователя

Часть 5. Межсетевой экран и другие средства фильтрации

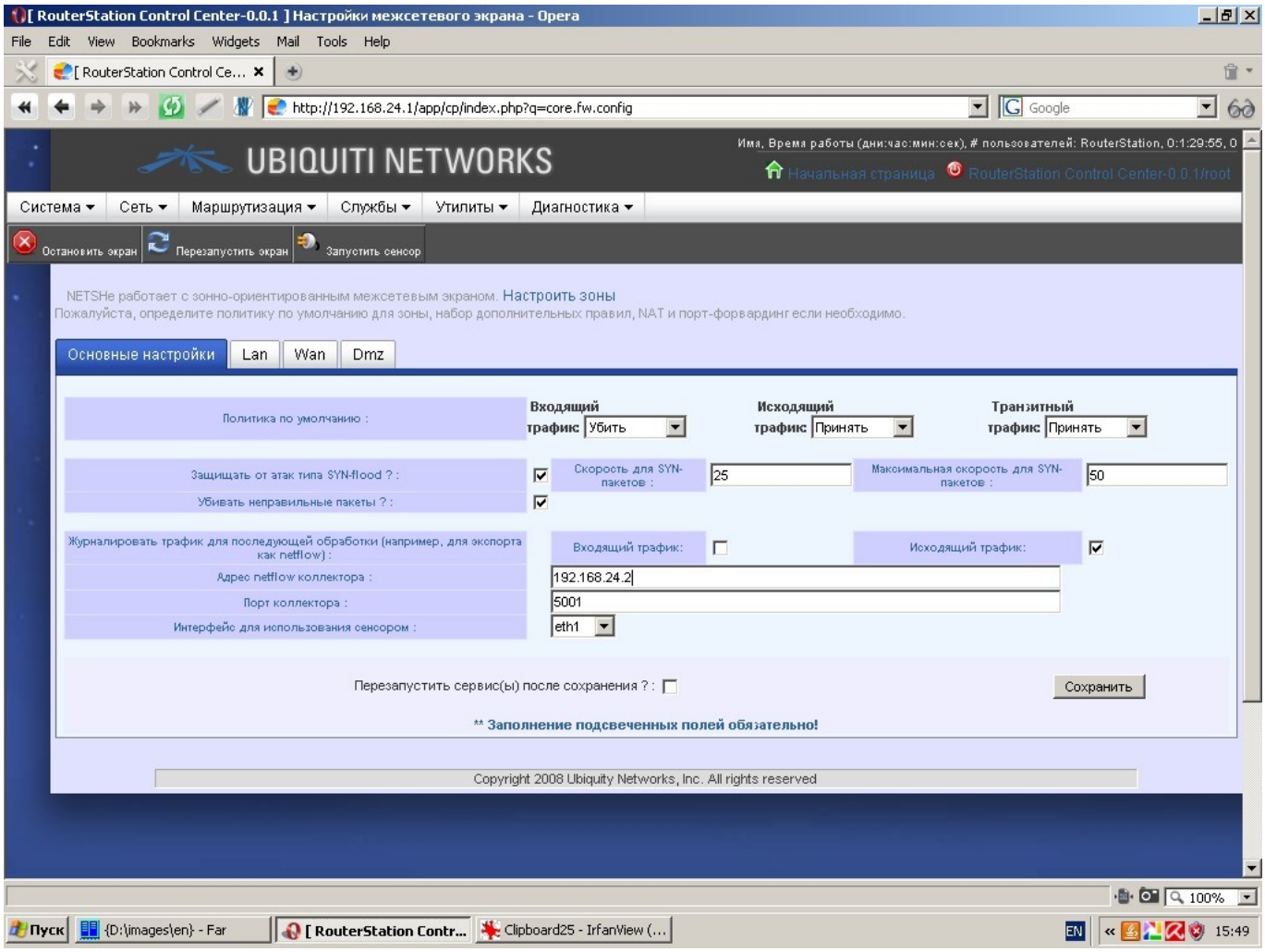
Станислав Корсаков, ООО «Нетше лаб»

Ярославль

Оглавление

Межсетевой экран в NETSHe

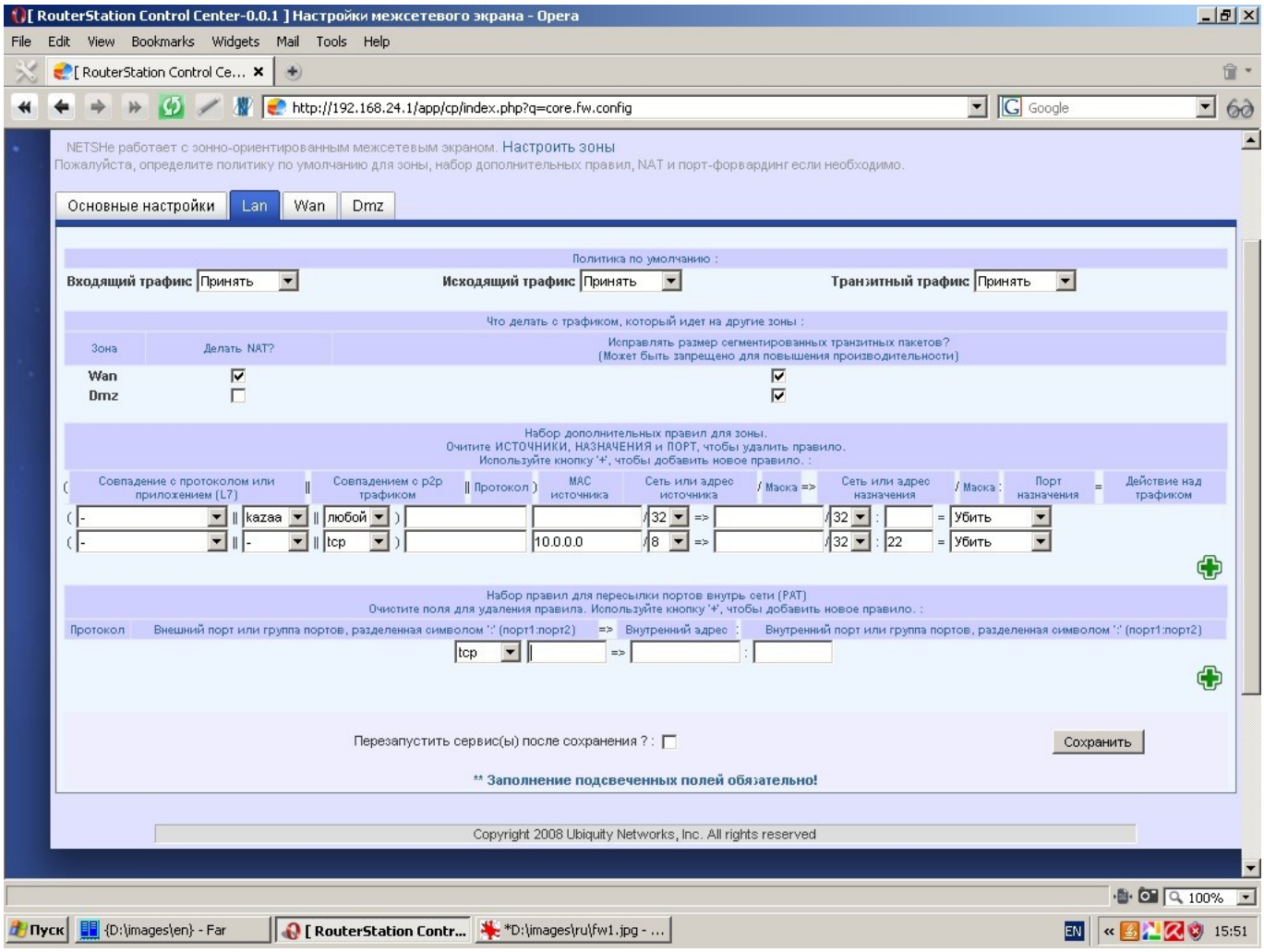
Система обладает весьма мощным межсетевым экраном и средствами управления им.



К встроенным функциям межсетевого экрана следует отнести:

- защиту от syn-flood атак;
- экспорт данных о потоке трафика, проходящем через экран в формате netflow v5
- Зональный принцип работы с автоматическим включением интерфейсов в соответствующую зону;
- Динамическая трансляция сетевых адресов (NAT);
- Статическая трансляция сетевых адресов и портов (SNAT/PAT);
- Задание умалчиваемых политик для всего экрана и, отдельно, для каждой из зон;
- Задание гибких правил для приема, отбрасывания, пересылки трафика на основании адресов источника и получателя, портов,

видов протокола (в том числе протоколов конкретных приложений (L7)), MAC-адресов источника и т. п. Правила задаются отдельно для каждой зоны;



Настройка межсетевого экрана.

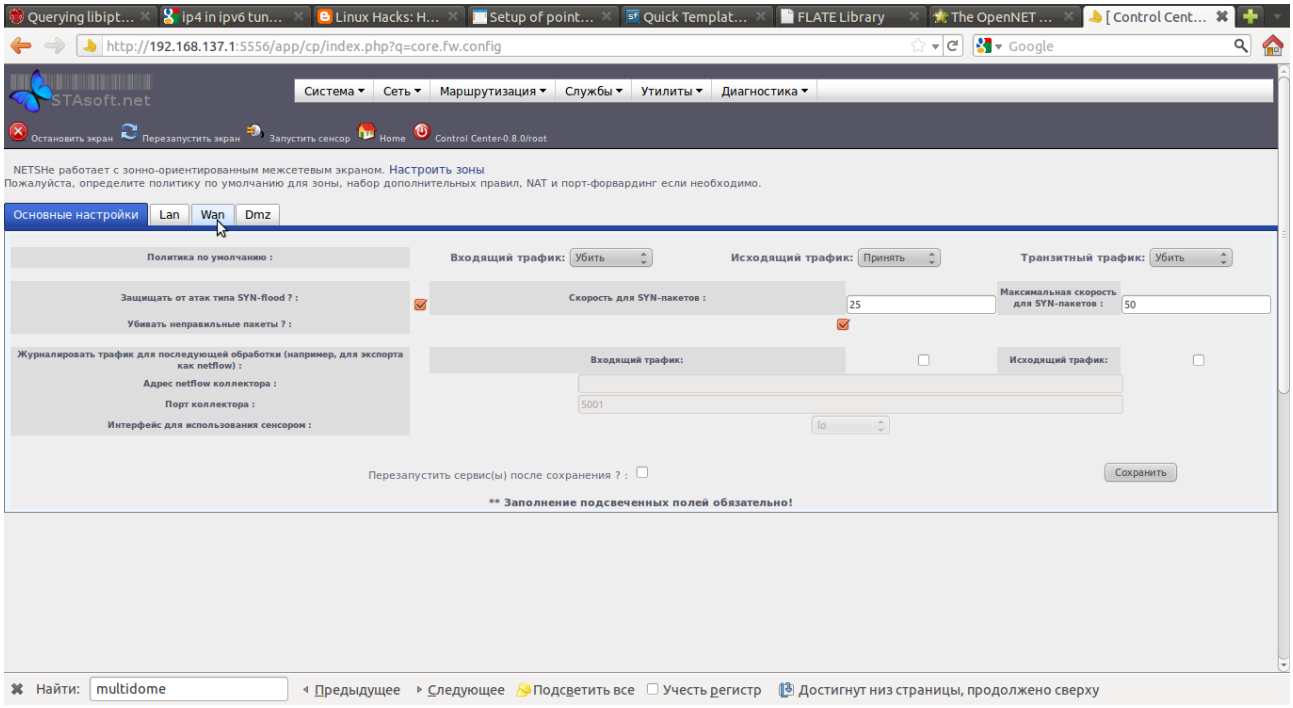
Межсетевой экран в NETSHe имеет определенные предустановки, реализующие выход в Интернет пользователям локальной сети и запрещающие доступ в локальную сеть и к службам на устройстве под управлением NETSHe снаружи.

Одной из часто возникающих задач является организация доступности какого-либо сервера, расположенного внутри сети, для внешних пользователей. Примером такой задачи может являться организация доступа к веб- или фтп-серверу.

Решается такая задачи путем пересылки (проброса) портов в межсетевом экране NETSHe.

Пересылка (проброс) портов внутрь сети в межсетевом экране NETSHe.

Для настройки пересылки (проброса) портов войдем в веб-интерфейс NETSHe и выберем управление межсетевым экраном («Сеть — Межсетевой экран»).



Выберем зону «Wan» в межсетевом экране и в разделе «Набор правил для пересылки портов внутрь сети» введем порт на внешних интерфейсах, который нужно пробросить внутрь сети (Например, 25), протокол, пакеты которого требуется пересылать внутрь сети (например, tcp), ip-адрес расположенного во внутренней сети компьютера (например, 192.168.1.2) и порт этого внутреннего компьютера, на который будет выполняться пересылка (например, 25).

Устанавливаем галочку «Перезапустить сервис после сохранения» и нажимаем кнопку «Сохранить».

Введенное нами правило сохраняется в списке правил для пересылки, а при поступлении tcp-пакета на 25 порт любого их наших внешних интерфейсов, такой пакет будет перенаправлен на 25-ый порт компьютера с адресом 192.168.1.2.

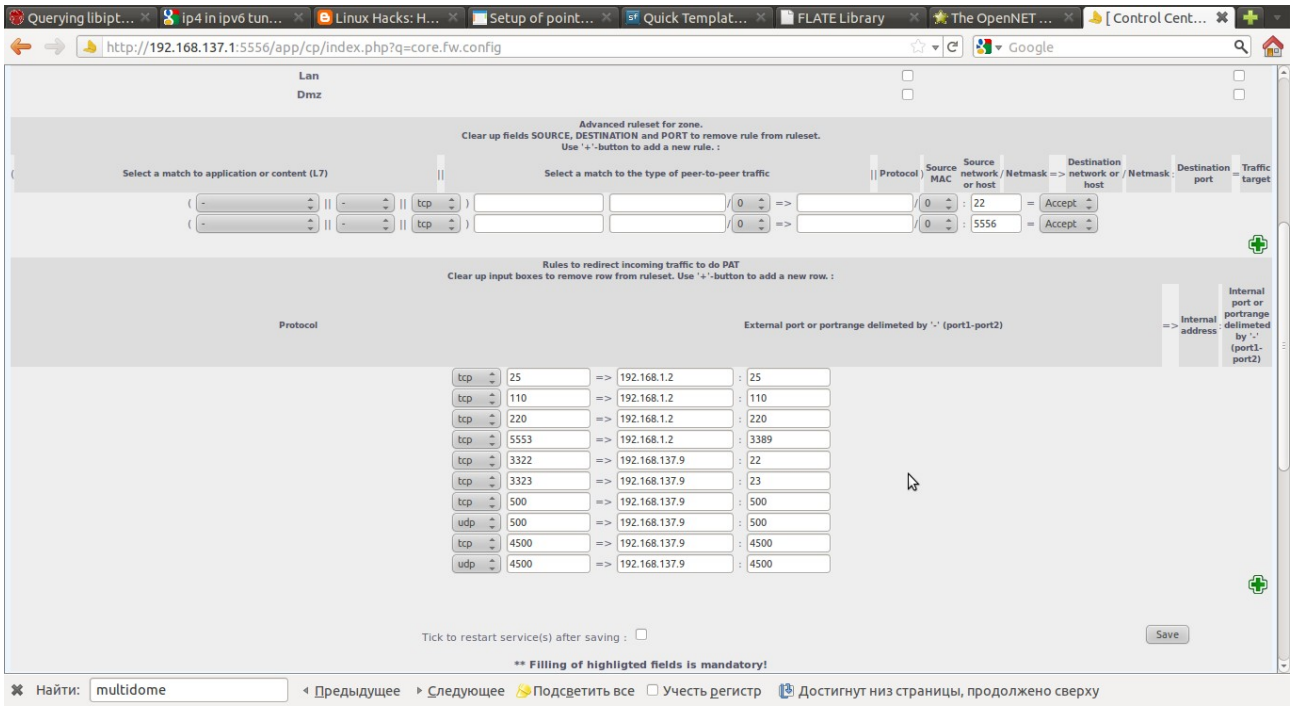
Приведенный нами пример относится к установке внутри сети SMTP-сервера и организации получения им почты извне.

Для установки FTP-сервера, нам потребовалось бы прописать пересылку портов 20 и 21.

При написании правил, следует учесть, что внешний и внутренний порты могут не совпадать. Так, можно замаскировать доступ по RDP (к RDP порту) конструкцией вида:

«Пересылать tcp-пакеты на внешний порт 5553 на внутренний адрес 192.168.1.2 порт 3389).

Примеры правил можно увидеть на иллюстрации ниже.



Доступ к веб-интерфейсу и SSH снаружи.

В ряде случаев, требуется разрешить доступ к службам на устройстве под управлением NETSHe снаружи. Например, к веб-интерфейсу и SSH (настоятельно не рекомендуется по соображениям безопасности).

Для этого, в веб-интерфейсе переходим к панели управления межсетевым экраном «Сеть — Межсетевой экран» и в настройках зоны «Wan» (как показано на иллюстрациях выше) в разделе «Набор дополнительных правил для зоны» вводим правила:

- Пакеты протокола tcp на внешний порт 22 принять
- Пакеты протокола tcp на внешний порт 5556 принять.

Устанавливаем галочку «Перезапустить сервис после сохранения» и нажимаем кнопку «Сохранить».

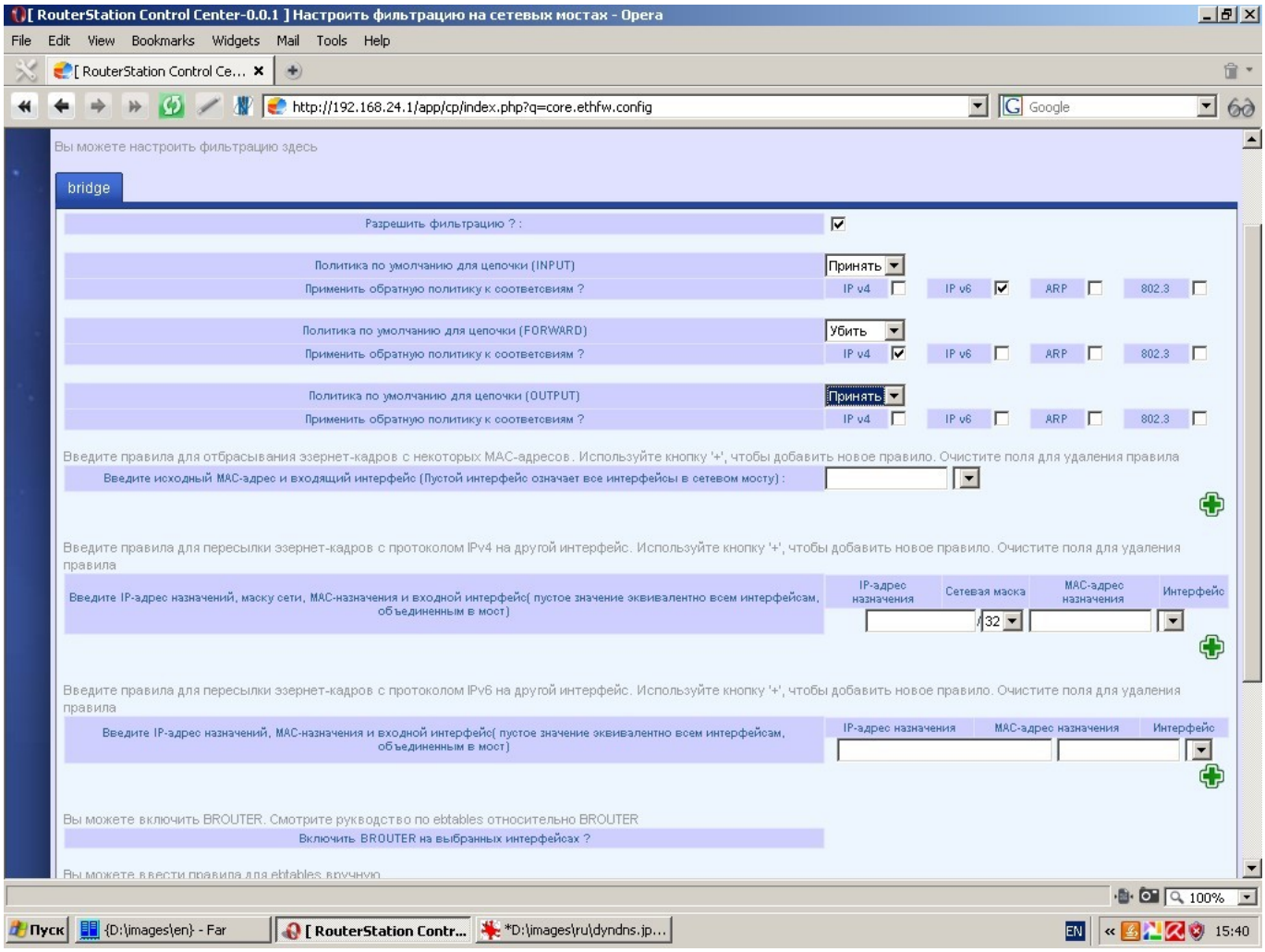
Веб-интерфейс и удаленный доступ стали возможными снаружи устройства.

Фильтрация эзернет-кадров

Система имеет средства для фильтрации трафика на уровне эзернет-кадров на сетевых мостах.

Внимание, Вы не можете использовать данную возможность, если у Вас в системе не определен хотя бы один сетевой мост.

Функция фильтрации трафика будет применяться только к трафику попадающему на данный сетевой мост. Кроме фильтрации, доступны функции перенаправления кадров с IP v4 и (или) IP v6 пакетами на другой Ethernet интерфейс; создания brouter.



Параметрами для настройки фильтрации являются:

- Политики по умолчанию;
- тип эзернет-кадров (например, 802.3 фрейм);
- содержимое эзернет-кадров (протокол IP v4 либо IP v6, ARP запрос);

- список MAC-адресов и (или) интерфейсов, для которых кадры следует отбросить.
- Список правил (адрес назначения/маска/MAC-адрес) для перенаправления IP пакетов на другие интерфейсы;
- список интерфейсов для создания brouter.

По вопросам создания, настройки и использования brouter смотрите документацию по *ebtables*.