SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Настройка межсетевого экрана

www.smart-soft.ru

1. Вступление

Компьютеры, подключенные к Интернету, могут подвергнуться несанкционированному доступу со стороны хакеров и прочих недоброжелателей. В Traffic Inspector Next Generation проблема несанкционированного доступа решается с помощью сетевого экрана.

2. Настройка

Настройки правил фильтрации доступны в разделе Межсетевой экран -> Правила.

2.1 Преднастроенные правила

Некоторые правила межсетевого экрана будут преднастроены.

- Правило Anti-Lockout Rule защищает администратора шлюза от потери доступа к web-интерфейсу. Данное правило разрешает доступ по протоколу HTTP (TCP/80), HTTPS (TCP/443) и SSH (TCP/22) на сам шлюз со стороны LAN-адаптера.
- Правило Default allow LAN to any rule разрешает неограниченный доступ со стороны LAN-адаптера для трафика, направленного в Интернет и на сам шлюз.

Учитывая преднастроенные правила, общая логика работы межсетевого экрана следующая: правила межсетевого экрана задаются отдельно для каждого из адаптеров, настроенных в системе. Правила располагаются в виде списка. Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету применено правило, то пакет не будет сверяться с оставшимися правилами в списке. Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (отбрасывается без индикации отправляющей стороне).

Порядок правил в списке, таким образом, имеет значение. В наиболее общем случае, запрещающие правила должны располагаться раньше (выше в списке) чем разрешающие.

По умолчанию, из внутренней сети разрешен любой доступ как на сам шлюз (LAN-адаптер шлюза), так и в Интернет. Любой трафик, являющийся ответным на тот, который был выпущен из внутренней сети, также свободно пропускается межсетевым экраном. Любое (несанкционированное из внутренней сети) обращение к шлюзу со стороны WAN-адаптера (Интернета) запрещено.

2.2 Разрешения трафика со стороны WAN-адаптера

Для примера, разрешим подключение к шлюзу Traffic Inspector NG со стороны WAN-адаптера по протоколу SSH.

Пройдите в раздел Межсетевой экран -> Правила, вкладка WAN. Кликните на значок + для создания нового правила. Создайте правило со следующими настройками:

Действие	Разрешение
Интерфейс	WAN
Версия TCP/IP	IPv4
Протокол	TCP
Источник	Любой
Диапазон портов источника	Любой – Любой
Назначение	WAN адрес
Диапазон портов назначения	SSH
Описание	Правило для разрешения подключений по SSH со стороны Интернета

Нажмите Сохранить для применения настроек.

Помимо собственно защиты компьютера от несанкционированных подключений, многие другие механизмы реализуются отчасти или полностью за счет межсетевого экрана, например: NAT, проброс портов, перенаправление трафика на прокси, DNS-форвардинг, ограничение пропуска трафика из / в гостевую сеть и прочие.

Настройка межсетевого экрана для данных нужд рассматривается в соответствующих инструкциях.