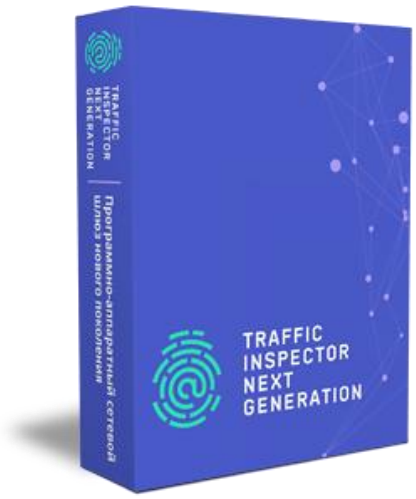

Универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений Traffic Inspector Next Generation — программно-аппаратный сетевой шлюз нового поколения для организации контролируемого доступа к интернету корпоративных компьютерных сетей и их защиты от внешних угроз. Относится к классу Unified Threat Management. Базируется на открытом коде проекта OPNsense.

Traffic Inspector Next Generation обеспечивает фильтрацию на разных уровнях модели OSI (сетевом, транспортном, прикладном) и управление через веб-интерфейс по защищенному HTTPS-подключению, а также по протоколу SSH с использованием терминального доступа. Решение разворачивается в роли шлюза на границе корпоративной сети и позволяет контролировать информационные потоки между локальной сетью и интернетом.

Модели в линейке:

- S100: для небольших домашних и офисных сетей. В качестве аппаратной платформы используются компьютеры x86-64 малого форм-фактора (152,4 x 152,4 мм).
- S500: для среднего бизнеса и государственных учреждений среднего размера.
- M1000: для крупного бизнеса и учреждений госсектора.
- L1000+: топовая модель для крупных коммерческих, государственных, образовательных организаций, учреждений здравоохранения, культуры, спорта и туризма.

  Аппаратная платформа моделей S500, M1000 и L1000+: стоечные серверы DEPO форм-фактора 1U.

Технические характеристики Traffic Inspector Next Generation:

- сетевой экран (Packet Filter) защищает шлюз и компьютеры пользователей от несанкционированного доступа извне, раздает интернет на пользователей, обеспечивает доступ к внутренним серверам из интернета;
- мониторинг сетевой активности и отчеты (NetFlow: отчет по сетевой активности, по наиболее популярным сетевым службам, по наиболее популярным IP-адресам. Веб-прокси: Domains (по посещенным доменам), URLs (по посещенным URL), Users (по пользователям, генерировавшим запросы на прокси), User IPs (по компьютерам, генерировавшим запросы на прокси). Утилиты RRDtool: отчет по состоянию интернет-канала, по использованию процессора, по использованию оперативной памяти, по количеству состояний трассировщика соединений сетевого экрана. Мониторинг загрузки сетевых интерфейсов в реальном времени. Журнал сетевого экрана. Системный журнал и syslog-ng);
- управление пропускной способностью интернет-доступа динамическим шейпером и приоритизацией трафика (ограничение максимальной скорости работы пользователя, резервирование выделенной полосы для трафика, распределение пропускной способности интернет-канала поровну между пользователями внутренней сети, приоритизация трафика приложения с помощью очередей для трафика, критичного к задержкам);
- различные виды VPN (OpenVPN, IPsec в туннельном режиме, L2TP/IPsec (IPSec в транспортном режиме), Tinc VPN, PPTP, PPPoE);
- кластеризация (использует протоколы CARP (VRRP), PFSYNC (синхронизация состояния межсетевых экранов), XMLRPC Sync (синхронизация прочих настроек шлюза);
- Connection Failover (в данном режиме шлюз переключается на запасные каналы доступа в интернет при выходе из строя основных, обеспечивая тем самым непрерывность доступа);
- система централизованного управления (Central Management System) распределенной инфраструктурой сетевых шлюзов (шлюз может быть мастер-узлом (master node) в центральном офисе и подчиненным узлом (slave node) в удаленном офисе);
- Captive Portal (в том числе с поддержкой SMS-идентификации);

- гибкая маршрутизация;
- прокси-сервер (Squid) поддерживает: HTTP, HTTPS, FTP, прозрачное проксирование, перехват и дешифрование SSL/TLS-соединений, кеширование веб-контента;
- фильтрация: по IP-адресам клиентов и сетям, по портам назначения, по типу браузера (User Agent), по типу контента (по MIME-типам), по общим белым и черным URL-спискам, по индивидуальным URL-спискам, назначаемым на доменного или локального пользователя или группу, по скачиваемым URL-спискам (SquidGuard), по категориям с помощью модуля NetPolice (в URL-списках допускается использование синтаксиса регулярных выражений);
- различные методы аутентификации (аутентификация по локальной базе, LDAP, RADIUS, Kerberos, привязка по IP- и MAC-адресам, двухфакторная аутентификация, ваучеры);
- Layer 7 — фильтрация (интеллектуальное распознавание протоколов прикладного (седьмого) уровня за счет сигнатурного анализа, используется для блокировки приложений вроде Skype и BitTorrent);
- шлюзовый антивирус (HTTP Antivirus Proxy + ClamAV) не требует установки на каждом клиентском компьютере, вместо этого устанавливается один раз на шлюзе и проверяет веб-трафик всех пользователей;
- среда: операционная система FreeBSD.

Срок действия лицензии — 5 лет, включает 1 год доступа к обновлениям и расширенной технической поддержке.

Решения компании «Смарт-Софт» защищают компьютерные сети «Газпрома», «Мегафона», Сбербанка, РЖД, «Роснефти», а также тысяч других компаний крупного, среднего и малого бизнеса и государственных организаций.