TRAFFIC INSPECTOR NEXT GENERATION®

Руководство пользователя

Модели S100, S200

для малых
и средних предприятий

SMART-SOFT®

Traffic Inspector Next Generation — универсальный шлюз безопасности, предназначенный для эффективной защиты внутренней сети от киберугроз. Разработан российской компанией Смарт-Софт (smart-soft.ru).

Модели S100, S200 для малых и средних предприятий просты в установке, не требуют привлечения специально обученного персонала и модификации имеющегося сетевого оборудования.

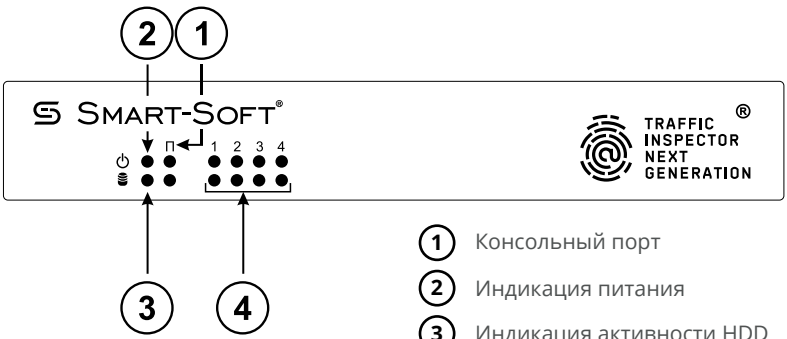
Основные функции моделей:

- контроль и фильтрация интернет-трафика (межсетевое экранирование);
- управление доступом сотрудников и клиентов к сети предприятия;
- предотвращение и выявление хакерских атак;
- защита внутренней сети от компьютерных вирусов и вредоносных программ;
- организация защищенного соединения между удаленными филиалами предприятия.

Все функции устройств представлены в онлайн-документации на сайте разработчика: smart-soft.ru/support/documentation.

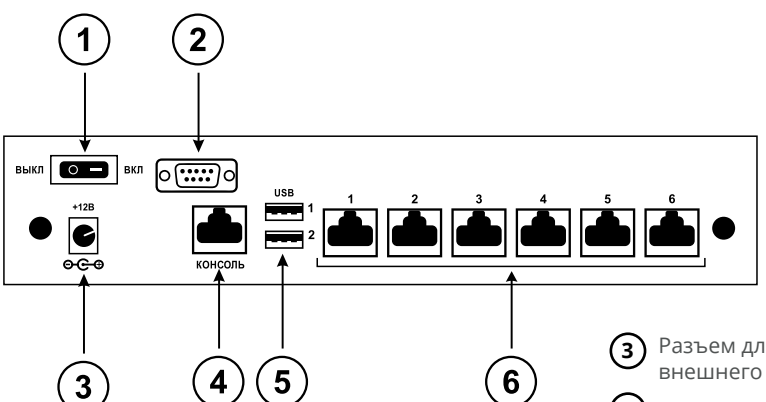
Внешний вид и подключение

Вид лицевой панели модели S100, S200

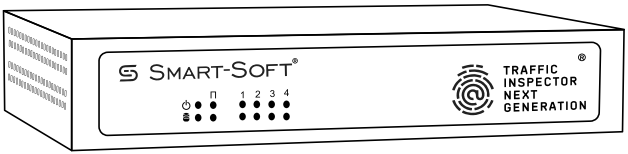


1. Консольный порт
2. Индикация питания
3. Индикация активности HDD
4. Индикация питания портов

Вид со стороны интерфейсов



1. Кнопка включения
2. Порт D-Sub (VGA)
3. Разъем для подключения внешнего блока питания (PS)
4. Консольный порт RS-232
5. USB порты (2 шт.)
6. Сетевые порты RJ-45 ports



1. Подключите маршрутизатор локальной сети (роутер) к сетевому порту № 1 на устройстве.

2. Подключите кабель интернет-провайдера к сетевому порту № 2.

3. Подключите питание.

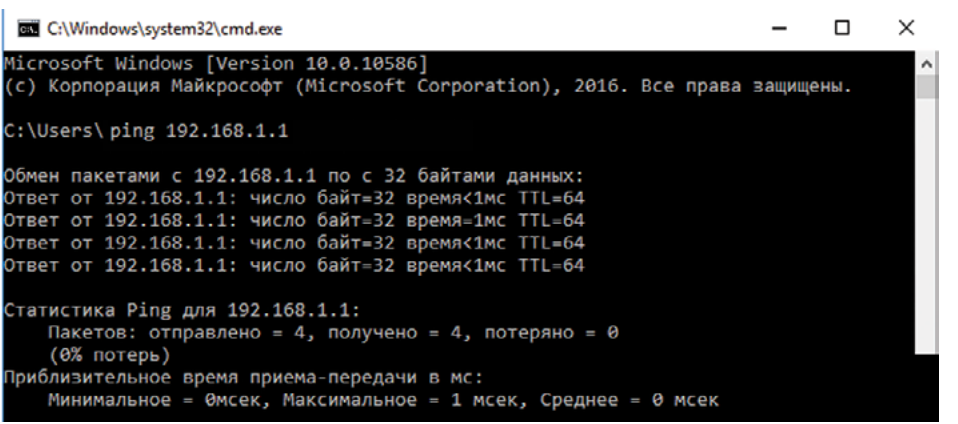
Устройство готово к работе. Далее необходимо выполнить начальные настройки.

Базовая настройка

Наиболее удобный способ управления Traffic Inspector Next Generation S100, S200 — через интернет-браузер.

Наберите в адресной строке браузера **192.168.1.1.**

Для проверки соединения компьютера с Traffic Inspector Next Generation выполните в командной строке команду ping (для операционной системы Windows нажать Win+R и набрать cmd):
ping 192.168.1.1



При успешном соединении браузер предупредит о наличии небезопасного соединения.

Игнорируйте сообщение (на примере браузера Chrome: нажмите «Дополнительные» — «Перейти на сайт 192.168.1.1 (небезопасно)»). В случае успеха появится окно входа в Traffic Inspector Next Generation.

Используйте логин **root**, пароль **ting.**

Шаг 1:
Запуск Мастера начальной настройки: раздел **«Система» –> «Мастер».**

В появившемся диалоге нажмите кнопку «Далее».

В диалоге «Система: Мастер: Основная информация» в разделе «Основная информация» можно изменить имя хоста (необязательно), указать домен (при использовании Microsoft AD), выбрать язык интерфейса.

Задайте DNS-серверы: первичный — обязательно, например DNS провайдера, вторичный — если имеется. Если DNS провайдера неизвестен, укажите DNS **8.8.8.8.**

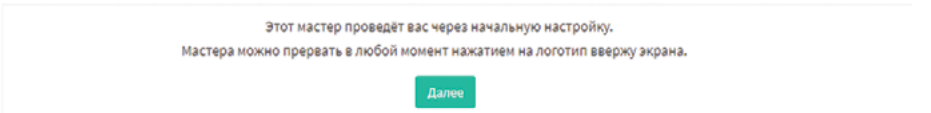
Раздел «Unbound DNS» рассчитан только на опытных пользователей.

ПРИМЕЧАНИЕ

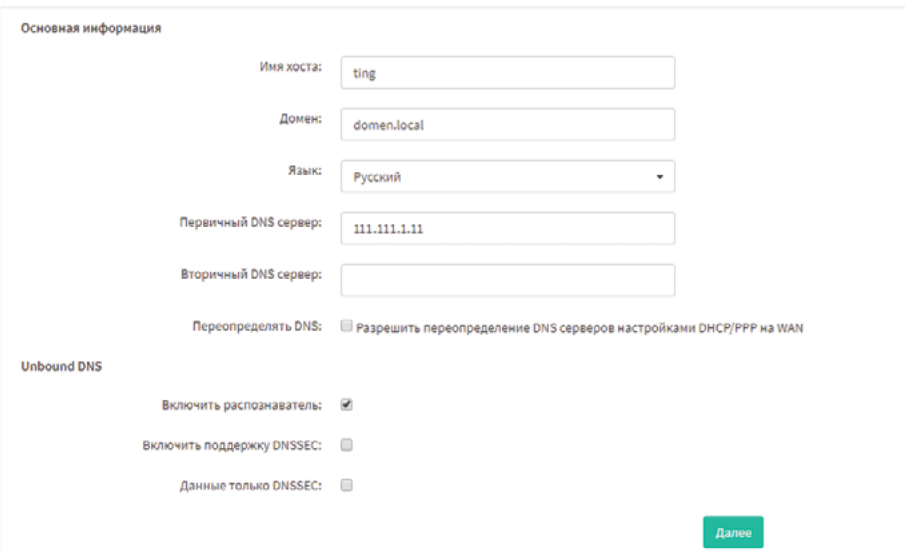
Устройство поддерживает DNS от Яндекса (dns.yandex.ru):

- «Безопасный»77.88.8.88 и 77.88.8.2 с антивирусом против мошеннических сайтов и вирусов;
- «Семейный» 77.88.8.7 и 77.88.8.3 с дополнительной функцией блокировки сайтов «для взрослых».

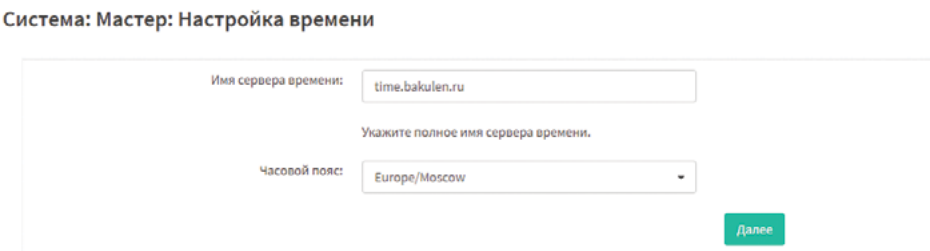
Система: Мастер: Мастер настройки TING



Система: Мастер: Основная информация



В диалоге «Система: Мастер: Настройка времени» в поле «Имя сервера времени» можно задать доменное имя сервера синхронизации времени (желательно) или использовать значение по умолчанию (отображение времени будет менее точным).



В диалоге «Система: Мастер: Конфигурация WAN-интерфейса» настройте интерфейс связи с провайдером интернета (WAN-интерфейс). Для этого необходимо установить тип взаимодействия, предоставляемый провайдером Интернета. Самый популярный тип, предоставляемый провайдером — DHCP. Данный тип установлен по умолчанию. В этом случае IP-адрес назначается автоматически внешним DHCP-сервером.

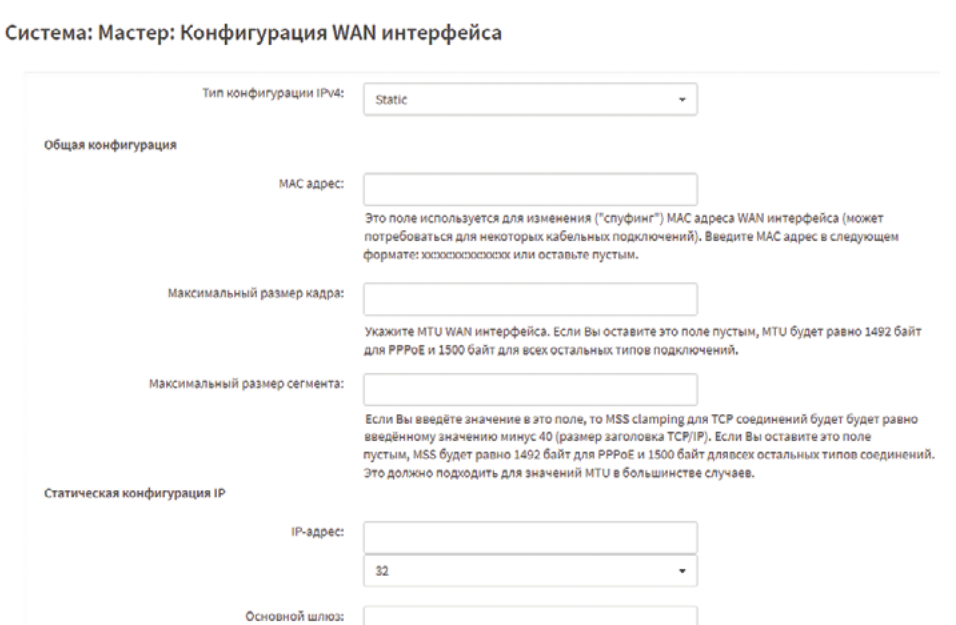
Все остальные типы связи рекомендованы для опытных пользователей.

Тип взаимодействия Static (IP-адрес назначается пользователем, им же назначаются обязательные параметры: префикс подсети, IP-адрес маршрутизатора по умолчанию), PPPoE (взаимодействие на уровне протокола канального уровня PPP, здесь можно указать параметры аутентификации на сервисе PPPoE и название сервиса), PPTP (защищенное соединение типа «точка — точка» с использованием туннельного протокола на уровне протокола IP, здесь можно задать параметры аутентификации, локальный IP-адрес для устройства, а также IP-адрес сервера PPTP).

Настройка параметров общей конфигурации — собственный MAC-адрес для WAN-интерфейса, собственное значение MTU (максимальная длина кадра) и MSS (максимальная длина сегмента) — рекомендована для опытных пользователей.

ПРИМЕЧАНИЕ

Если провайдер предоставляет IP-адреса из диапазона частных сетей, в настройках WAN-интерфейса необходимо снять галочку с пункта «Блокировать частные сети».



Конфигурация DHCP-клиента

Имя хоста для DHCP:

Значение этого поля отправляется в качестве идентификатора DHCP-клиента и имени хоста при запросе аренды адреса. Некоторые поставщики услуги Интернет могут потребовать это значение (для идентификации клиента).

Конфигурация PPPoE

Имя пользователя PPPoE:

Пароль PPPoE:

Имя сервиса PPPoE:

PPPoE соединение по требованию: Включить режим «Соединение по запросу»

Это опция заставляет интерфейс работать в режиме соединение-по-требовани, позволяя Вам иметь виртуальное постоянное соединение. Интерфейс настроен, но реальное соединение отложено до того момента, когда будет обнаружен исходящий трафик.

Таймаут отключения PPPoE:

Если в течение указанного количества секунд не передается ни одного квалифицирующего исходящего пакета, соединение прерывается. Время простоя, равное нулю, отключает эту функцию.

Конфигурация PPTP

Имя пользователя PPTP:

Пароль PPTP:

Локальный IP адрес PPTP:

32

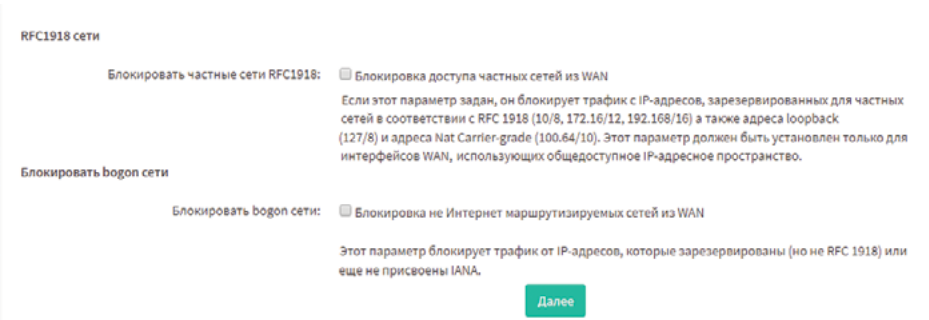
IP адрес сервера PPTP:

Соединение PPTP по требованию: Включить режим «Соединение по запросу»

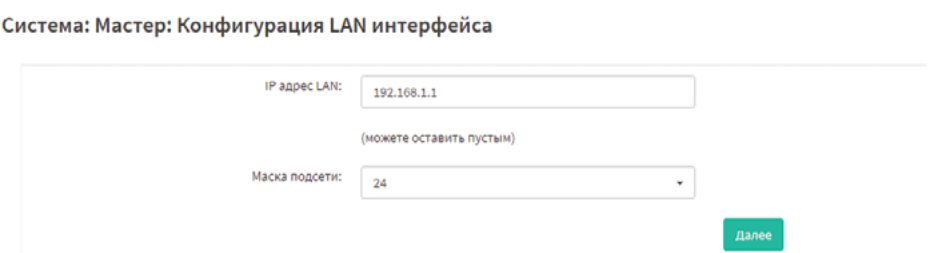
Это опция заставляет интерфейс работать в режиме соединение-по-требовани, позволяя Вам иметь виртуальное постоянное соединение. Интерфейс настроен, но реальное соединение отложено до того момента, когда будет обнаружен исходящий трафик.

Таймаут отключения PPTP:

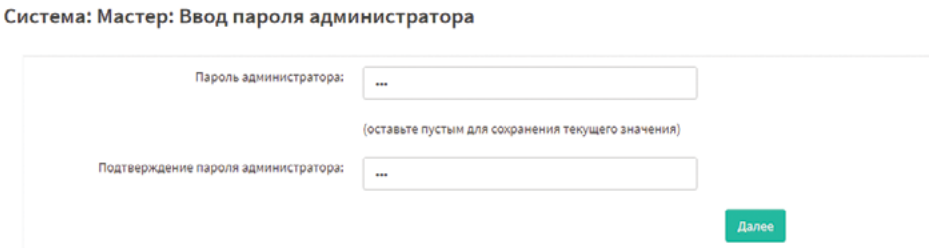
Если в течение указанного количества секунд не передается ни одного квалифицирующего исходящего пакета, соединение прерывается. Время простоя, равное нулю, отключает эту функцию.



В диалоге «Система: Мастер: Конфигурация LAN-интерфейса» пользователь может изменить параметры интерфейса LAN, IP-адрес и маску подсети. Рекомендуется оставить параметры по умолчанию. Данные параметры необходимо изменять только опытным пользователям.

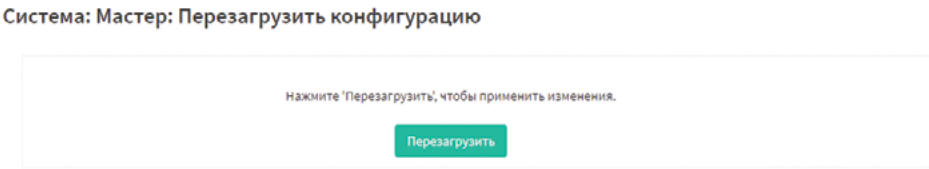


В диалоге «Система: Мастер: Ввод пароля администратора» пользователь может сменить пароль пользователя root.



ПРИМЕЧАНИЕ

В целях безопасности исходный пароль необходимо заменить на собственный.



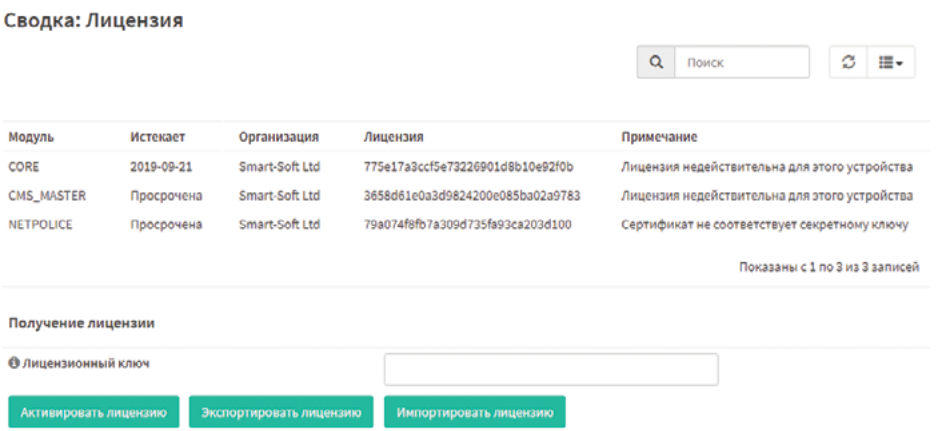
После перезагрузки системы будет открыт доступ к сети Интернет и репозиторию плагинов Traffic Inspector Next Generation.

Шаг 2:
Установка лицензии: «Главное меню» -> «Сводка» -> «Лицензия».

Если лицензия в форме хеш-последовательности (длинная строка цифр и букв), введите ее в поле «Лицензионный ключ» и нажмите «Активировать лицензию».

Если лицензия в виде текстового файла, нажмите «Импортировать лицензию», выберите файл и нажмите «Активировать лицензию».

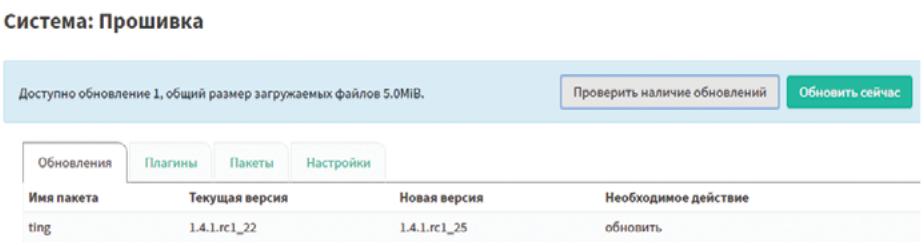
После того как лицензия активирована, она отображается в списке лицензий*.



* При покупке Traffic Inspector Next Generation Лицензионный ключ уже предустановлен. Ввод Лицензионного ключа может понадобиться в дальнейшем. Например, при сбросе до заводских настроек (сохраняйте ключ перед сбросом).

Шаг 3:
Обновление программного обеспечения: «Главное меню» -> «Система» -> «Прошивка» -> «Проверить наличие обновлений».

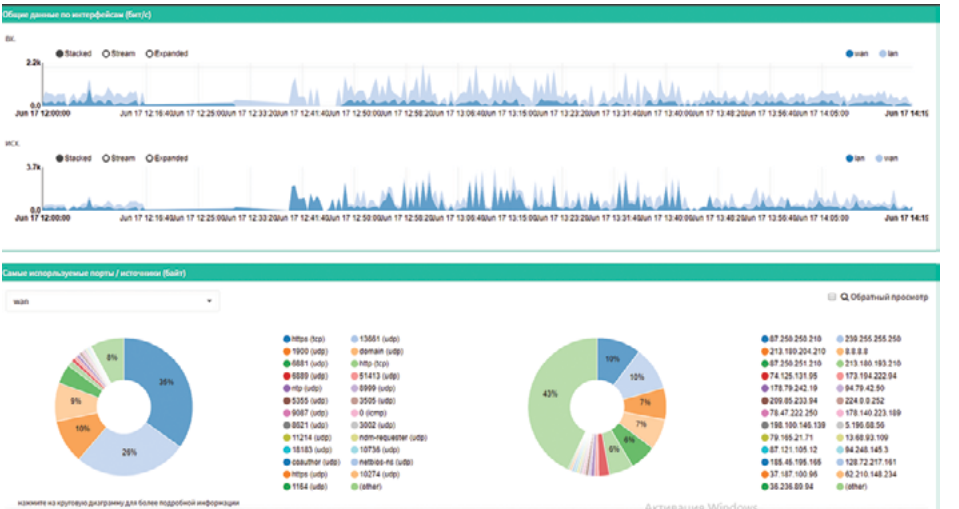
Если будет обнаружена более новая версия ПО, нажмите «Обновить сейчас», дождитесь завершения обновления и перезапуска системы.



Базовые настройки завершены. В устройстве активированы основные функции.

Функции в базовых настройках:
- DHCP сервер - выделение IP адресов устройствам в локальной сети;
- межсетевой экран - предоставление доступа в сеть Интернет на основании правил межсетевого экранирования по умолчанию.

Для просмотра статистики сетевого трафика необходимо включить функцию Netflow: «Главное меню» -> «Создание отчетов» -> «NetFlow»



Отчет по сетевой статистике доступен в разделе «Анализ» и содержит данные о том, какой компьютер на какой адрес обращался, по какому порту/сервису и сколько данных было передано по каждому взаимодействию.

Также система формирует отчеты с распределением трафика по портам назначения, сетевым службам, IP-адресам назначения и т.п.

Для выгрузки данных в разделе «Анализ» предусмотрена вкладка «Экспорт».

Для продвинутого использования устройства необходимо произвести дополнительные настройки Traffic Inspector Next Generation.

Воспользуйтесь инструкциями по настройке на сайте Смарт-Софт: https://www.smart-soft.ru/support/documentation/handbook/ting/

или видеоуроками:
https://www.smart-soft.ru/support/documentation/video_ting/

Функции, требующие дополнительной настройки и установки плагинов:

- Управление доступом сотрудников и клиентов к сети Интернет как для незащищенного, так и защищенного соединения.

  Для настройки перейдите в раздел «Межсетевой экран и NAT»: https://www.smart-soft.ru/support/documentation/handbook/ting/firewall_nat.html и в раздел «Веб-прокси» руководства пользователя на сайте Смарт-Софт: https://www.smart-soft.ru/support/documentation/handbook/ting/proxy.html.

- Предотвращение и выявление хакерских атак - сканирование сетевого трафика на предмет выявления вредоносных сигнатур.

  Для настройки перейдите в раздел «Система обнаружения / предотвращения вторжений» руководства пользователя на сайте Смарт-Софт: https://www.smart-soft.ru/support/documentation/handbook/ting/idsips.html.

- Защита внутренней сети от компьютерных вирусов и вредоносных программ.

Для настройки перейдите в подраздел «Антивирусная проверка трафика» раздела «Веб-прокси» руководства пользователя на сайте Смарт-Софт: https://www.smart-soft.ru/support/documentation/handbook/ting/av.html.

- Организация защищенного соединения между удаленными филиалами предприятия - VPN каналы.

  Для настройки перейдите в раздел «VPN» руководства пользователя на сайте Смарт-Софт: https://www.smart-soft.ru/support/documentation/handbook/ting/vpn.html.

Технические характеристики Traffic Inspector Next Generation S100, S200

Класс решения	UTM
Платформа	OPNsense
Межсетевой экран	есть
Система обнаружения и предотвращения вторжений	основана на коде и сигнатурах Suricata, а также поддерживает правила ET Open, интегрирована с SSL Blacklist (SSLBL) и трекером Feodo.
Организация шифрованных VPN-каналов	между филиалами, партнерскими организациями, удаленными сотрудниками и центральным офисом. Благодаря интеграции с СКЗИ «МагПро Криптопакет» вы сможете организовывать шифрованные по ГОСТ VPN-каналы связи. Это важно, если вы работаете с государственными учреждениями

Двухфакторная аутентификация пользователей	есть
Функция прокси-сервера	есть
Правила доступа	разные для разных категорий сотрудников: • разрешенные или запрещенные сайты («черные» и «белые» списки) для разных категорий пользователей • автоматическая блокировка нежелательного или вредоносного контента • блокировка приложений правилами глубокой пакетной инспекции
Дополнительные модули	• модуль антивирусной защиты Anti-Virus powered by Kaspersky обеспечивает проверку трафика (HTTP(S) и FTP), проходящего через прокси-сервер и почтовый шлюз программы Traffic Inspector Next Generation; • фильтр контента NetPolice фильтрует сайты по категориям и их содержимому, не позволяет получить доступ к определенным сайтам или услугам сети Интернет (например, к вредному и опасному для детей и подростков контенту).
Аппаратные характеристики	
Модель	APU2C4
Процессор	AMD Embedded G series GX-412TC
Сеть	3 x 1 GbE

Порты GbE RJ45 [10/100/1000 Мбит/с]	3 i210AT NICs
Порты USB	2 USB 3.0
Консольный порт	1 RS-232
Устройство хранения данных	30 GB
Оперативная память	4 GB DDR3-1333 DRAM
CPU / ядро	1 GHz quad Jaguar core with 64 bit and AES-NI support
Виртуальные интерфейсы	4093
Размеры	
Высота * ширина * длина (мм)	30 * 168 * 157
Форм фактор	6 x 6» (152,4 x 152,4 мм)
Вес (кг)	0,45
Рабочая среда	
Питание	12 V
Максимальный ток	1,5 A
Потребление электроэнергии (усредненное)	18 W
Рабочая температура	0 до +45 °C
Температура хранения	-20 до +70 °C
Влажность	10-90% без конденсации

Онлайн-инструкция

http://www.smart-soft.ru/support/documentation

Служба технической поддержки

Если вы столкнулись с проблемой при работе или настройке устройства, обратитесь в службу технической поддержки.

Тел.: +7 (495) 77-55-991 (доб. 6401)
E-mail: info@smart-soft.ru

УСЛУГА НАСТРОЙКИ TRAFFIC INSPECTOR NEXT GENERATION «ПОД КЛЮЧ»

Смарт-Софт оказывает услуги по настройке и конфигурированию Traffic Inspector Next Generation: наш специалист удаленно подключится к вашей сети, произведет установку решения и настройку его функций согласно вашим требованиям.

Для заказа услуги свяжитесь с нами.

Тел.: +7 (495) 77-55-991
E-mail: info@smart-soft.ru

О разработчике

Компания Смарт-Софт – ведущий российский разработчик комплексных систем защиты информации и управления доступом в интернет для бизнеса, госсектора, образовательных и медицинских учреждений, учреждений культуры - многофункционального межсетевого экрана и системы обнаружения (предотвращения) вторжений Traffic Inspector, универсального шлюза безопасности (UTM) и системы обнаружения (предотвращения) вторжений Traffic Inspector Next Generation.

Собственные решения на основе уникальных программных алгоритмов полностью соответствуют требованиям российского законодательства в области защиты информации.

Решения компании Смарт-Софт входят в Единый реестр российских программ для электронных вычислительных машин и баз данных и защищают компьютерные сети Газпрома, Мегафона, Сбербанка, РЖД, Роснефти, а также тысяч других компаний крупного, среднего и малого бизнеса и государственных организаций.

За 19 лет работы Смарт-Софт сформировала партнерскую сеть, состоящую более чем из 2500 российских и международных компаний.