SMART-SOFT®

БЕЗОПАСНАЯ СЕТЬ С TRAFFIC INSPECTOR NEXT GENERATION

СМАРТ-СОФТ, 2022

Traffic Inspector Next Generation

Универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений

UTM-устройство **Traffic Inspector Next Generation** обеспечит защиту вашей сети благодаря таким высококачественным функциям как система предотвращения вторжений, виртуальные частные сети, двухфакторная аутентификация, Captive portal и фильтрующий веб-прокси. Опциональная функция кластера высокой доступности - залог стабильной и бесперебойной работы за счет автоматического переключения на запасные каналы и синхронизации состояния между участниками кластера.
Обеспечьте защиту и непрерывную работу вашей сети.

Пропускная способность сетевого экрана – 850 Мбит/с, до 75 000 пакетов в секунду.

Пропускная способность системы предотвращения вторжений – до 750 Мбит/с Блокировка сайтов по цифровым отпечаткам SSL сертификатов.

Быстрая фильтрация по различным характеристикам, включая Layer 7 – фильтрацию.

Достаточная емкость внутренней памяти для хранения логов и отчетов — до 1 ТБ.

Защита доступа в интернет. Фильтрующий прокси (с поддержкой инспекции SSL). Captive Portal с различными типами аутентификации.

Поддержка двухфакторной аутентификации во всей системе. Совместимо с Google Authenticator.

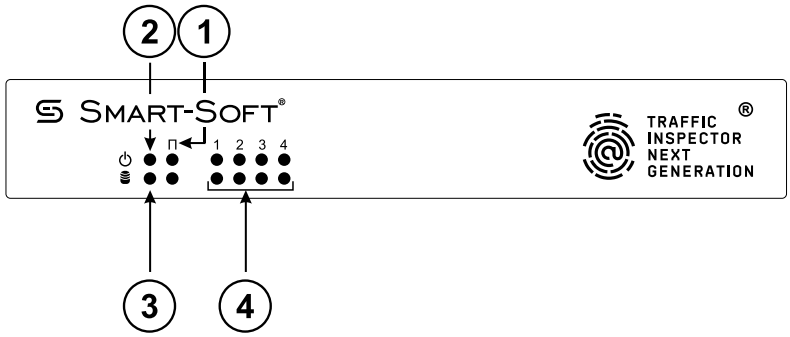
Криптографическая защита VPN-соединений (перспективная разработка).

Аппаратное обеспечение

СЕРИИ S100, S200

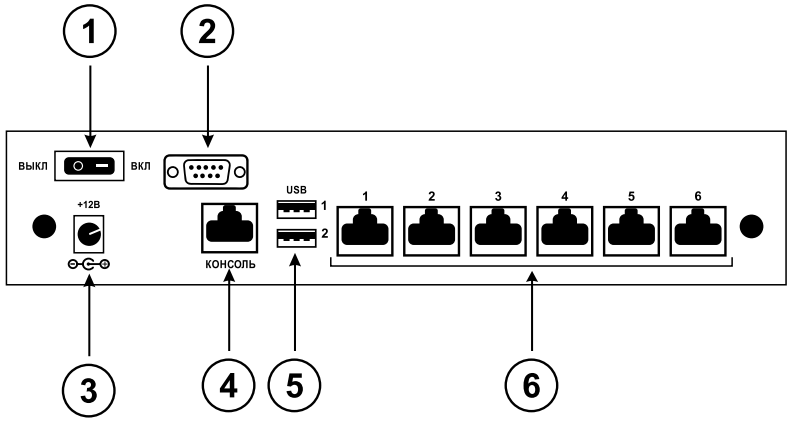
Форм-фактор 1 U

Вид лицевой панели моделей S100, S200

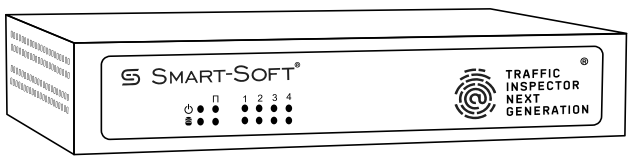


1. Консольный порт
2. Индикация питания
3. Индикация активности HDD
4. Индикация питания портов

Вид со стороны интерфейсов моделей S100, S200



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.

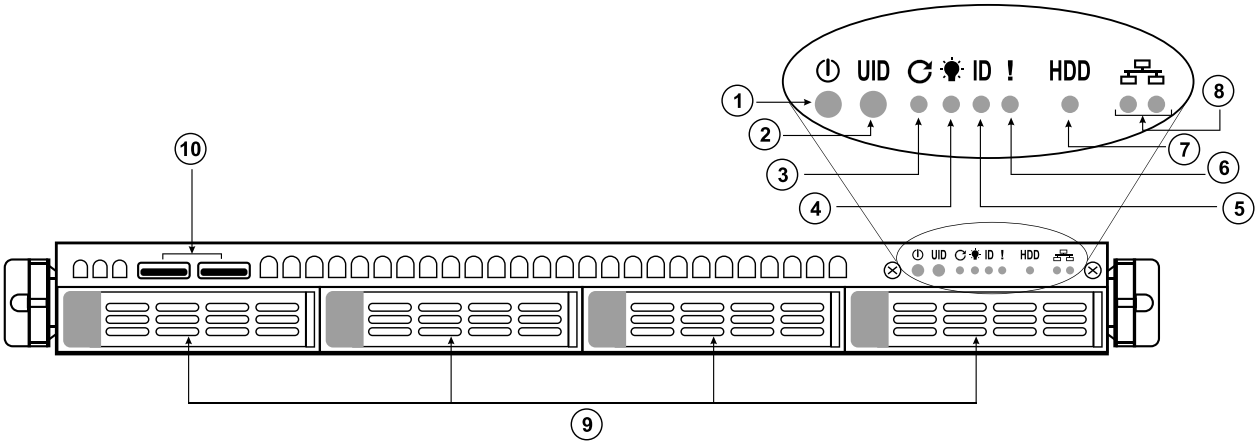
Устройство готово к работе. Далее необходимо выполнить начальные настройки.

Аппаратное обеспечение

СЕРИИ S500, M1000 и L1000+

Аппаратная платформа: стоечные серверы форм-фактора 1U.

Вид лицевой панели моделей: S500, M1000, L1000+

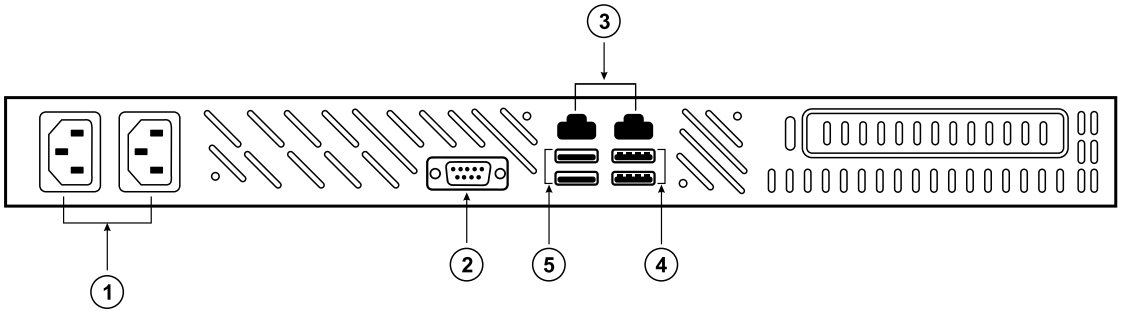


1. Кнопка включения питания
2. Кнопка управления индикатором обозначения изделия
3. Кнопка сброса системы (Reset)
4. Индикатор статуса питания
5. Индикатор обозначения изделия (ID) - позволяет однозначно идентифицировать в стойке конкретное изделие при большом количестве управляемых удаленно однотипных изделий.
6. Не используется и не подключен
7. Индикатор активности жесткого диска SATA
8. Индикаторы статуса интегрированных сетевых контроллеров
9. Корзины для жестких дисков
10. Разъемы USB 2.0

Аппаратное обеспечение

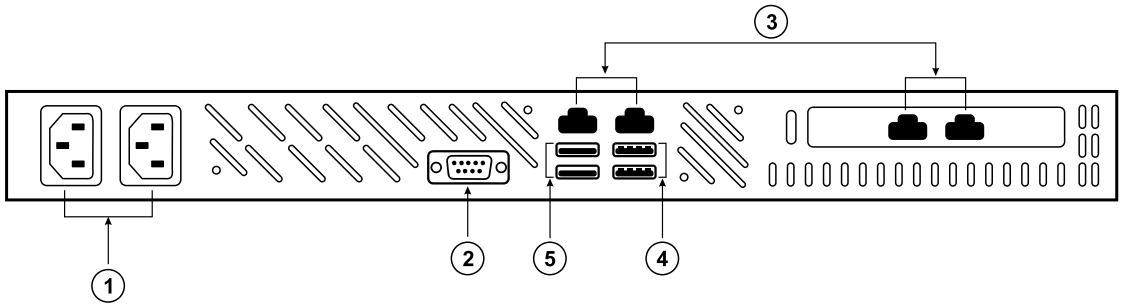
СЕРИИ S500, M1000 и L1000+

Вид модели S500 со стороны интерфейсов



1. Разъем подключения питания для изделия
2. VGA-порт
3. Сетевые разъемы RG-45
4. Разъемы USB 3.0
5. Разъемы USB 2.0

Вид модели M1000 и L1000+ со стороны интерфейсов



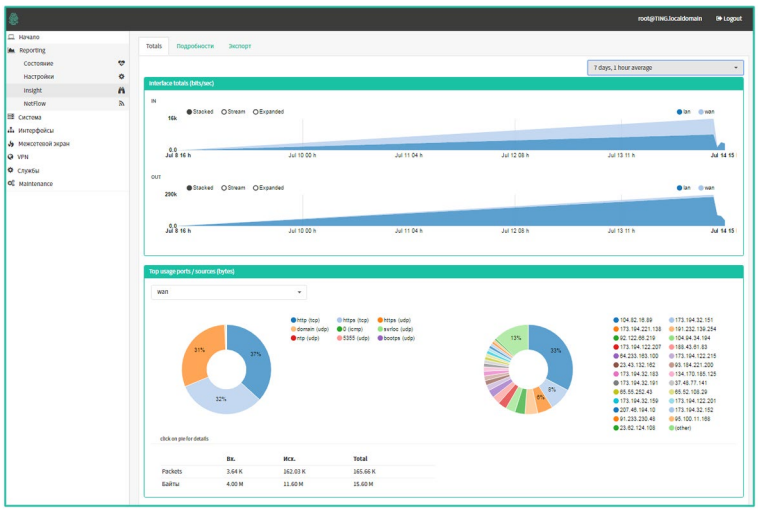
1. Разъем подключения питания для изделия
2. VGA-порт
3. Сетевые разъемы RG-45
4. Разъемы USB 3.0
5. Разъемы USB 2.0

С помощью Ethernet-кабеля подключите Ethernet-адаптер (1) устройства Traffic Inspector Next Generation к сети организации.

С помощью Ethernet-кабеля подключите Ethernet-адаптер (3) устройства Traffic Inspector Next Generation к сети провайдера.

Программное обеспечение

Универсальное решение с богатым функционалом.



Traffic Inspector Next Generation – динамично развивающийся программно-аппаратный сетевой шлюз нового поколения для организации контролируемого доступа к интернету корпоративных компьютерных сетей и их защиты от внешних угроз, разрабатываемый российской компанией «Смарт-Софт». Относится к классу Unified Threat Management. Характерная особенность решения – богатый функционал, базирующийся на открытом программном обеспечении.

Весь функционал доступен из графического интерфейса с удобной навигацией. С помощью нашего решения вы можете с легкостью защитить свою сеть – воспользуйтесь встроенной системой предотвращения вторжений с функцией проверки SSL-сертификатов и двухфакторной аутентификацией при подключении мобильных пользователей.

Благодаря технологии сетевой статистики NetFlow и анализатора данных Insight вы всегда будете иметь полное представление о трафике, передающемся через ваше устройство.

Бизнес

Защита сетевой инфраструктуры вашего бизнеса и безопасность сетевых соединений.

Для внедрения и сопровождения Traffic Inspector Next Generation не потребуются высокооплачиваемые IT-специалисты в штате, не нужна интеграция различных модулей в одну систему — вы получаете решение «все в одном», начиная с контекстного сетевого экрана и заканчивая системой обнаружения / предотвращения вторжений. Шейпер поможет улучшить производительность сети и приоритезировать VOIP-трафик.

Отели, рестораны, кафе

Компаниям индустрии гостеприимства и питания подойдет функционал Captive Portal, позволяющий организовать как платный, регулируемый по времени, так и бесплатный доступ в интернет для своих гостей.

Постояльцы отелей и посетители кафе и ресторанов могут выходить в интернет с помощью ваучера (карты), который приобретается или получается бесплатно на ресепшен. Такие ваучеры легко генерируются в Captive Portal по мере необходимости. Также можно настроить бесплатный доступ для гостей к Wi-Fi сети заведения через аутентификацию посредствам SMS.

Учреждения образования

Разграничивайте и делите поровну пропускную способность интернет-канала между учащимися, преподавателями, гостями учебного учреждения, запрещайте доступ детей к нежелательным веб-ресурсам (сайтам для взрослых, сайтам-рассадникам вирусов) с помощью функции веб-фильтрации. Данная функция легка в настройке, вы можете использовать как свои списки, так и наши базы запрещенных сайтов, включая списки NetPolice.

Работа в командировках

Traffic Inspector Next Generation принесет пользу вашему бизнесу, даже если вы или ваши сотрудники в пути. VPN на базе OpenVPN, IPsec или WireGuard поддерживает удаленных пользователей и двухфакторную аутентификацию. Возможность экспорта конфигурации превратит настройку клиента OpenVPN в минутное дело. ГОСТ VPN позволяет организовать защищенное взаимодействие с устройствами удаленных сотрудников, соблюдая требования российского законодательства.

Филиалы, удаленные офисы и сотрудники

VPN на базе технологий IPsec и SSL VPN идеально подходит для организации взаимодействия с филиалами и удаленными офисами. WireGuard открывает возможности использования самой современной криптографии, а ГОСТ VPN позволяет организовать защищенное соединение между географически распределенными объектами и выполнить требования российского законодательства. Примеры и подробные инструкции по настройке доступны онлайн и помогут начать работать с VPN быстро и эффективно.

Государственные организации и операторы персональных данных

Высокопроизводительная защита корпоративных сетей от киберугроз доступна государственным учреждениям всех уровней, включая образовательные и медицинские учреждения, муниципалитеты, министерства и контролирующие ведомства.

Traffic Inspector Next Generation включен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Программное обеспечение

Обзор функциональных возможностей

Traffic Inspector Next Generation (версия 1.10.0 на базе OPNsense 22.1.1)*

Межсетевой экран

- Фильтрация по:
  - Адресу источника
  - Адресу назначения
  - Протоколам
  - Портам
  - Операционной системе (фингерпринтинг ОС)
- Каждое правило может задавать свои настройки ограничения одновременных соединений
- Каждое правило может определять свои настройки журналирования трафика
- Нормализация пакетов
- Возможность выключить фильтрацию пакетов и работать в режиме чистого маршрутизатора
- Сбор и отображение статистики для всех правил межсетевого экрана
- Отображение автоматических правил межсетевого экрана в веб-интерфейсе

Организация политик

- Поддержка псевдонимов / алиасов
  - Для IP-адресов
  - Диапазонов портов
  - Доменных имен (полностью определенное доменное имя)
- Интерфейсные группы
  - Возможность создания зон безопасности с помощью правил, ссылающихся на интерфейсные группы
- Категории правил
  - Легкий доступ к наборам правил
- Поддержка GeoIP (определение страны)

Гибкий контроль таблицы состояний

- Настраиваемый размер таблицы состояний
- Каждое правило может задавать свои настройки
  - Ограничения одновременных подключений от клиента
  - Ограничения состояний для конкретного хоста
  - Ограничения на количество новых соединений в секунду
  - Таймаута для состояний соединения
  - Режима работы с соединениями
- Режимы работы с соединениями
  - Keep (режим отслеживания состояния соединения)
  - Sloppy (менее строгий режим отслеживания состояния соединения)
  - Modulate (генерация высококачественных Initial Sequence Number)
  - Synproxy (режим защиты от атаки типа TCP YSN Flood)
  - None (режим работы без отслеживания состояния соединения)
- Оптимизация работы с соединениями
  - Normal (нормальный режим подходит для большинства сетей)
  - High latency (режим высокой задержки – подходит для спутниковых каналов связи)
  - Aggressive (агрессивный режим – соединения истекают быстрее, тратится меньше памяти)
  - Conservative (консервативный режим - соединения истекают медленнее, тратится больше памяти)

Аутентификация

- Удаленные серверы
  - LDAP
  - RADIUS
  - Kerberos (только для прокси-сервера) для Active Directory и FreeIPA
  - NTLM (только для прокси-сервера)
- Встроенные возможности
  - Локальный менеджер пользователей
  - Ваучеры / карты
  - FreeRadius (плагин)
  - Прозрачная аутентификация по технологии единого входа для пользователей домена

Авторизация

- Веб-интерфейс
  - Локальный менеджер пользователей

Аккаунтинг

- FreeRadius
- Ваучеры / карты

Двухфакторная аутентификация

- Поддержка TOTP (одноразовых паролей с ограничением по времени)
- Поддержка Google Authenticator
- Поддержка 2FA-аутентификации в:
  - Captive Portal
  - Веб-прокси
  - VPN
  - Веб-интерфейсе
  - SSH / консоль

Сертификаты

- Удостоверяющий центр
  - Создание или импортирование удостоверяющего центра
  - Создание или импортирование сертификатов
- Плагин Let's Encrypt
  - Автоматически разворачиваемый доверенный удостоверяющий центр

Поддержка 802.1Q VLAN

- Максимальное поддерживаемое число VLAN-сетей – 4096

Агрегирование каналов и переключение при сбое

- Переключение при сбое
- Балансировка нагрузки
- Циклический алгоритм (Round Robin)
- Технология Ether Channel (FEC) от Cisco
- Протокол LACP из стандарта IEEE 802.3AD

Поддержка других типов интерфейсов

- Мостовые интерфейсы
- Generic Tunnel Interface / GIF (различные виды тунелирования IPv4/6 в IPv4/6)
- GRE (универсальные протокол инкапсулирования от Cisco)

Трансляция сетевых адресов (NAT)

- Поддержка NAT Reflection (обращение к серверам из внутренней сети по публичным IP-адресам)
- Логирование правил NAT
- Исходящий NAT

Шейпер трафика

- Ограничение пропускной способности
- Разделение пропускной способности
- Приоритезация трафика
- Критерии совпадения правил
  - Протокол
  - Адрес источник
  - Адрес назначения
  - Порт
  - Направление

Полная поддержка технологии Universal Plug & Play

Dynamic DNS

- Выбор сервиса Dynamic DNS из списка
- Произвольно настраиваемый сервис
- Поддержка RFC 2136

DNS Форвардер
- Переопределения для хостов
- Переопределения для доменов

DNS Сервер
- Переопределения для хостов
  - Для ресурсных записей типа A
  - Для ресурсных записей типа MX
- Списки доступа
- Поддержка DNSSEC
- Протокол шифрования DNS-трафика (dnscrypt-proxy), который позволяет защитить DNS-запросы от подмены и перехватов

DNS Фильтрация
Поддержка OpenDNS

DHCP Сервер
- Поддержка IPv4 и IPv6
- Поддержка режима ретрансляции
- Поддержка BOOTP-опций

MultiWAN
- Балансировка нагрузки
- Переключение на запасной канал при сбое основного канала
- Псевдонимы / алиасы

Балансировка нагрузки
- Распределение входящей сетевой нагрузки между несколькими обслуживающими серверами во внутренней сети (HAProxy)

Network Time Server
- Поддержка Pulse Per Second источника
- Поддержка GPS-источника

Система обнаружения / предотвращения вторжений
- Работа в режиме inline (устройство, выполняющее функцию, находится на пути трафика, а не в стороне)
- Предопределенные правила
  - Черные списки SSL-сертификатов
  - Feodoro Tracker
  - Geolite2 Country IP
  - Emerging Threats ETOpen
- Блокировка сайтов по цифровым отпечаткам SSL сертификатов
- Автообновление правил с помощью планировщика cron

Layer 7 - фильтрация
- системо-независимый API для использования userland-приложениями, которые используют низкоуровневые механизмы захвата пакетов (libpcap и BPF)
- блокировка трафика, распознанного с помощью nDPI и запрещённого в настройках.
- правила для отчёта и блокировки приложений по отдельным подсетям.
- каждое правило может работать в режиме только отчёта или режиме блокировки.

Captive Portal
- Сценарии использования
  - Гостевая сеть
  - BYOD (Мобильное рабочее место)
  - Wi-Fi-доступ в отелях и кемпингах
  - Управление шаблонами
  - Поддержка нескольких зон
- Аутентификаторы
  - Работает со всеми поддерживаемыми в системе аутентификаторами
  - Без аутентификации (только экран приветствия)
  - Аутентификация с помощью SMS с поддержкой групп пользователей.
  - Отчётность по траффику пользователей на прокси.
- Менеджер ваучеров
  - Поддержка нескольких баз данных ваучеров
  - Экспортирование ваучеров в формат CSV
- Таймауты и распознавание зарегистрированных пользователей
- Управление пропускной способностью
  - Доступно с помощью шейпера
- Обход портала
  - По белым спискам IP- и MAC-адресов
- Отчеты в реальном времени
  - Топ-лист по IP-адресам с наибольшим использованием пропускной способности канала
  - Активные сессии
  - Оставшееся время
  - Интерфейс программирования REST

Виртуальные частные сети
- IPsec
  - В режиме «сеть - сеть»
  - В режиме «узел - сеть» (подключение удаленных сотрудников)
- OpenVPN
  - В режиме «сеть - сеть»
  - В режиме «узел - сеть» (подключение удаленных сотрудников)
  - Экспорт конфигурации для легкой настройки клиента
  - OpenVPN client export API для автоматизации процесса выдачи клиентских сертификатов для OpenVPN
- Tinc
  - Маршрутизация в режиме полносвязной топологии
- ZeroTier (плагин)
  - VPN, SDN и SD-WAN
- PPTP (унаследованное ПО)
- L2TP (унаследованное ПО)
- Плагин ГОСТ-VPN на базе OpenVPN с использованием ГОСТ-шифрования
- Поддержка WireGuard

Высокая доступность
- Переключение на запасной узел в кластере высокой доступности
- Синхронизация таблицы состояния соединений между узлами кластера
- Синхронизация настроек между узлами кластера

Кеширующий прокси
- Поддержка нескольких интерфейсов
- Режим прозрачного проксирования
- Создание списка разрешенных сайтов для варианта «запрещено всё» в режиме прозрачного проксирования
- Перехват и дешифровка HTTPS-соединений (SSL Bump)
- Списки контроля доступа
- Черные списки ресурсов
- Управление трафиком
- Поддержка скачиваемых черных списков
- ICAP (поддержка внешних антивирусов)
- Аутентификация SSO для Active Directory и FreeIPA с возможностью отключения Basic-аутентификации
- Поддержка NTLM-аутентификации
- Привязка пользователя к IP/MAC-адресу
- Запись логов в БД, гибкая отчётность по доменам, URL, пользователям, IP-адресам и т.д.
- Логирование трафика пользователей OpenVPN с привязкой к пользователю
- Гибкая настройка правил пользователей и групп (приоритеты, чёрные/белые списки, исключения SSL Bump, правила ICAP, маршрутизация на разные интернет-каналы)
- Фильтрация по категориям ресурсов NetPolice
- Интеграция с FreeIPA
- Возможность формирования списка исключений для доступа к сайтам, имеющим собственные (самоподписанные) SSL-сертификаты. Список сайтов (доменов) устанавливается администратором вручную при настройке универсального шлюза безопасности
- Поддержка мультипроцессорных и многоядерных систем

- Возможность принудительного ограничения пропускной способности прокси-сервера для отдельных пользователей
- Поддержка возможностей фильтрации через SkyDNS: использование ns-серверов для настройки единых ограничений для всех пользователей

Антивирусная проверка
- Поддержка интеграции с внешними антивирусами с помощью ICAP
- ClamAV (встроенный антивирус, работающий со Squid через плагин C-ICAP)
- Плагин антивируса Касперского
- Антивирусная защита почтового трафика

Обратный прокси
- Распределение входящей сетевой нагрузки между несколькими обслуживающими серверами во внутренней сети (HAProxy)
- Веб-сервер Nginx

Анонимность в сети
- Анонимизация исходящих подключений для приложений
- Анонимизация входящих подключений для серверов (анонимные службы)
- Tor

Резервное копирование и восстановление
- История изменений настроек
- Резервное копирование файлов
- Сохранение резервной копии в облако
- API backup export – автоматизация работы с резервными копиями

SNMP
- Мониторинг и ловушки

Диагностика
- Статус перезагрузки фильтров
- Информация по сетевому экрану
- Топ по активным пользователям
- Таблицы сетевого экрана
  - Псевдонимы / алиасы
  - Bogon-сети (немаршрутизируемые в Интернете адреса)
- Текущие открытые сокеты
- Просмотр состояний всех соединений
- Сброс таблицы состояний
- Общие данные по состояниям соединений
- Технология Wake on LAN (пробуждение компьютера при получении пакета по сети)
- ARP-таблица (кэш протокола преобразования адресов)
- Просмотр данных в DNS
- NDP-таблица (кэш протокола обнаружения соседей)
- Утилита PING
- Захват пакетов
- Сканирование портов
- Трассировка маршрутов

Мониторинг
- Агент Zabbix (плагин)
- Monit (плагин)
  - Проактивный мониторинг системы

Усовершенствованная система отчетов
- Анализатор потоков Insight
  - Полностью интегрирован в решение
  - Детальная агрегация данных
  - Графическая репрезентация данных
  - Поддержка поиска и кликабельность
  - Экспорт в формат CSV
- Здоровье системы
  - Работа с собираемыми данными по циклическому алгоритму
  - Возможность выбора и масштабирования
  - Возможность экспорта
- Графики трафика
  - Мониторинг трафика в реальном времени
- Hardware widget – предоставление сведений об аппаратной платформе

Мониторинг сети
- NetFlow Exporter
  - Версия 5 и 9
  - Поставляет данные в Insight
- Сканирование сети сканером безопасности
- ntopng - мониторинг трафика и сбор потоков

Система управления пакетами
- Поддержка установки в виртуальную машину
  - VMware Tools
  - Утилиты Xen Guest
- Легкий апгрейд
  - Предупреждение о перезагрузке при базовом апгрейде
- Возможность выбора зеркала обновлений
- Возможность переустановки пакета
- Запрет на обновление конкретного пакета
- Возможность аудита
  - Проверка установленных пакетов на наличие уязвимостей
- Поддержка плагинов

Интерфейс программирования REST
- Поддержка списков контроля доступа

Central Management System
- Централизованная панель управления несколькими узлами на головном узле

Родительский контроль
- Возможность переключения YouTube в безопасный семейный режим

Импорт пользователей и групп из многофункционального межсетевого экрана Traffic Inspector

Онлайн документация
- Документация в свободном доступе на русском языке, с поддержкой поиска

Поддержка русского языка
- Полная поддержка русского языка в интерфейсе
- Поддержка кириллических доменов во всех подсистемах
- Документация на русском

*** Примечание.** Состав функций может быть изменен без дополнительного уведомления. Уточняйте состав функций текущей версии у работников отдела продаж (sales@smart-soft.ru).

Traffic Inspector Next Generation Light

- Исключена система обнаружения и предотвращения вторжений (IDS/IPS)
- Исключен функционал контроля приложений (L7-фильтрация)

Traffic Inspector Next Generation FSTEC (версия 1.0.2)**

- Аудит контрольных сумм файлов базовой системы, ядра и пакетов ПО
- Защита от несанкционированных изменений конфигурации системы
- Отключены встроенные антивирусы
- Отсутствует сканер безопасности сети
- Отсутствует система обнаружения / предотвращения вторжений

**** Примечание:** функциональные возможности ФСТЭК-версии ограничены по сравнению с перечнем функциональных возможностей версии 1.9.0. Уточняйте состав функций ФСТЭК-версии у работников отдела продаж (sales@smart-soft.ru).

Компания Смарт-Софт осуществляет поддержку Traffic Inspector Next Generation FSTEC до 01.06.2022, поэтому для его текущих пользователей сохранена возможность использования приобретенного ранее продукта. Получение нового сертификата ФСТЭК для Traffic Inspector Next Generation планируется в 2022 году.

Технические характеристики

Производительность и возможности

Малый бизнес, небольшие организации.

	Traffic Inspector Next Generation S100	Traffic Inspector Next Generation S200
Количество учетных записей	до 100	до 200
Базовая конфигурация	**DEPO Stream 1040C2X**	**DEPO Stream 1060CX**
Процессор	Intel® Celeron™ N3060 (2-Core, 1.6GHz, 2MB)	Intel® Celeron™ J1900 (4-Core, 2.0GHz, 2MB)
Оперативная память	8GB DDR3L SO-DIMM 1.35V	8GB DDR3L SO-DIMM 1.35V
Дисковый массив	1000GB SATA HDD 2.5”	1000GB SATA HDD 2.5”
Кабели	Консольный кабель RJ-45 -> COM (RS-232)	Консольный кабель RJ-45 -> COM (RS-232)
Сетевая карта	Четыре порта 1GbE RJ-45 (Intel i211)	Шесть портов 1GbE RJ-45 (Intel i211)
Механические опции	Крепёж для установки диска 2.5”	Крепёж для установки диска 2.5”
Гарантия и дополнительный сервис	Стандартная ONS1S - на месте эксплуатации сервера 1 год (при наличии СЦ в городе)	Стандартная ONS1S - на месте эксплуатации сервера 1 год (при наличии СЦ в городе)

Крупный и средний бизнес, большие организации.

	Traffic Inspector Next Generation S500
Количество учетных записей	От 100 до 500
Базовая конфигурация	**DEPO Storm 3450A2**
Процессор	Intel® Xeon® Silver 4208 [8 ядер, 16 потоков, 2.1 ГГц, 11 МБ кэш, 85 Вт]
Оперативная память	32 ГБ: 2 x 16 ГБ DDR4 ECC REG
Контроллер	Интегрированный: 4x SATA-III + 8x SATA-III + 2x SATA III (Rear)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковая корзина	Корзина горячей замены 8 x SAS/SATA + 4 x SAS/SATA/NVME без экспандера
Конфигурация платы	DP, C621, 24DIMM, 12xSATA3, 2 PCIE 3.0 x24, 1 PCIE 3.0 x8, 2RSC, 2 M.2, noLAN, 2USB, VGA, COM, IPMI 2.0 & iKVM с выделенным портом
Слот расширения	Сетевая карта, 4 порта, 1 Гбит/с, RJ-45
Слот расширения	Сетевая карта, 2 порта, 10 Гбит/с, SFP+, трансиверы 1 Гбит/с, RJ-45
Модуль удаленного управления	Интегрированный IPMI 2.0 + KVM-over-LAN с выделенным портом
Блок питания	Сдвоенный блок питания 800 Вт (2x800 Вт)
Комплект для монтажа в стойку	Рельсы с безвинтовым креплением, регулируемая длина 673мм ~ 924мм
Гарантия и дополнительный сервис	Стандартная CAR1S - 1 год с обслуживанием в СЦ

	Traffic Inspector Next Generation M1000
Количество учетных записей	От 500 до 1000
Базовая конфигурация	**DEPO Storm 3450A2**
Процессор	Intel® Xeon® Silver 4210R [10 ядер, 20 потоков, 2.4 ГГц, 13.75 МБ кэш, 100 Вт]
Оперативная память	64 ГБ: 2 x 32 ГБ DDR4 ECC REG
Контроллер	Интегрированный: 4x SATA-III + 8x SATA-III + 2x SATA III (Rear)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковая корзина	Корзина горячей замены 8 x SAS/SATA + 4 x SAS/SATA/NVME без экспандера
Конфигурация платы	DP, C621, 24DIMM, 12xSATA3, 2 PCIE 3.0 x24, 1 PCIE 3.0 x8, 2RSC, 2 M.2, noLAN, 2USB, VGA, COM, IPMI 2.0 & iKVM с выделенным портом
Слот расширения	Сетевая карта, 4 порта, 1 Гбит/с, RJ-45
Слот расширения	Сетевая карта, 2 порта, 10 Гбит/с, SFP+, трансиверы 1 Гбит/с, RJ-45
Модуль удаленного управления	Интегрированный IPMI 2.0 + KVM-over-LAN с выделенным портом
Блок питания	Сдвоенный блок питания 800 Вт (2x800 Вт)
Комплект для монтажа в стойку	Рельсы с безвинтовым креплением, регулируемая длина 673мм ~ 924мм
Гарантия и дополнительный сервис	Стандартная CAR1S - 1 год с обслуживанием в СЦ

	Traffic Inspector Next Generation L1000+
Количество учетных записей	Более 1000
Базовая конфигурация	**DEPO Storm 3450A2**
Процессор	2 x Intel® Xeon® Silver 4210R [10 ядер, 20 потоков, 2.4 ГГц, 13.75 МБ кэш, 100 Вт]
Оперативная память	128 ГБ: 4 x 32 ГБ DDR4 ECC REG
Контроллер	Интегрированный: 4x SATA-III + 8x SATA-III + 2x SATA III (Rear)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковый массив	1 x 1000 ГБ SATA-накопитель (7200 об/мин)
Дисковая корзина	Корзина горячей замены 8 x SAS/SATA + 4 x SAS/SATA/NVME без экспандера
Конфигурация платы	DP, C621, 24DIMM, 12xSATA3, 2 PCIE 3.0 x24, 1 PCIE 3.0 x8, 2RSC, 2 M.2, noLAN, 2USB, VGA, COM, IPMI 2.0 & iKVM с выделенным портом
Слот расширения	Сетевая карта, 4 порта, 1 Гбит/с, RJ-45
Слот расширения	Сетевая карта, 2 порта, 10 Гбит/с, SFP+, трансиверы 1 Гбит/с, RJ-45
Модуль удаленного управления	Интегрированный IPMI 2.0 + KVM-over-LAN с выделенным портом
Блок питания	Сдвоенный блок питания 800 Вт (2x800 Вт)
Комплект для монтажа в стойку	Рельсы с безвинтовым креплением, регулируемая длина 673мм ~ 924мм
Гарантия и дополнительный сервис	Стандартная CAR1S - 1 год с обслуживанием в СЦ

5 фактов о компании Смарт-Софт

Российский разработчик

Разработка и техническая поддержка продуктов - в России.

Старше Facebook

Первые строчки кода разработчики Смарт-Софт написали в 2003 году.

1 975 лицензий

Максимальное количество лицензий, которое было приобретено одним заказчиком единовременно.

5 компьютеров

Самая маленькая локальная сеть, которую защищает решение от Смарт-Софт.

Анадырь

Самый восточный город России, в котором работает клиент Смарт-Софт. География внедрений решений Смарт-Софт включает все регионы России: от Анадыря на востоке до Калининграда на западе и от Певека на севере до Дербента на юге.

КОНТАКТЫ

+7 (800) 511-05-81, +7 (495) 775-59-91

info@smart-soft.ru

www.smart-soft.ru