TRAFFIC INSPECTOR NEXT GENERATION®

Безопасная сеть с Traffic Inspector Next Generation



SMART-SOFT®

Traffic Inspector Next Generation



TRAFFIC INSPECTOR NEXT GENERATION ®



Межсетевой экран следующего поколения **(Next-Generation Firewall, NGFW) 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.

Сетевой экран (Packet Filter) защищает шлюз и компьютеры пользователей от несанкционированного доступа извне, раздает интернет на пользователей, обеспечивает доступ к внутренним серверам из интернета.

Система обнаружения и предотвращения вторжений (IDS/IPS) распознает источники атак и атакуемые машины по определенным сигнатурам сетевого трафика и эффективно «очищает» его.

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

Достаточная емкость внутренней памяти для хранения логов и отчетов.

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.

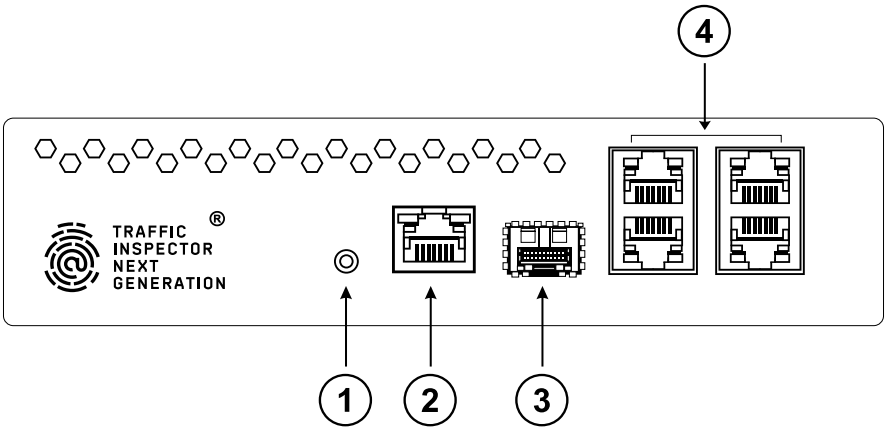
Криптографическая защита VPN-соединений.

Аппаратное обеспечение

СЕРИЯ S100

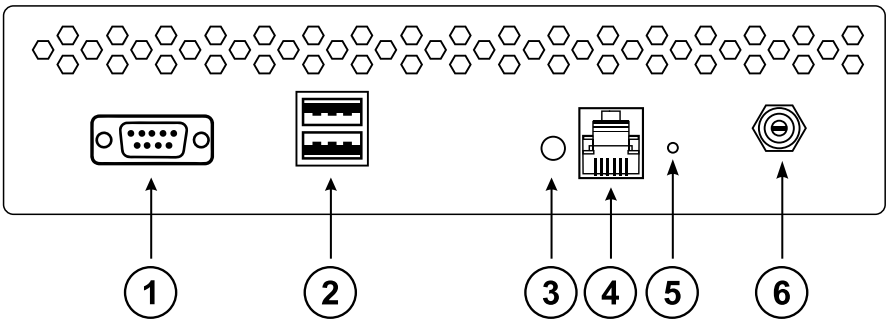
NP-1002i

Вид лицевой панели



1. Индикатор состояния
2. COM
3. Ethernet (SFP)
4. Ethernet (RJ45)

Вид со стороны интерфейсов



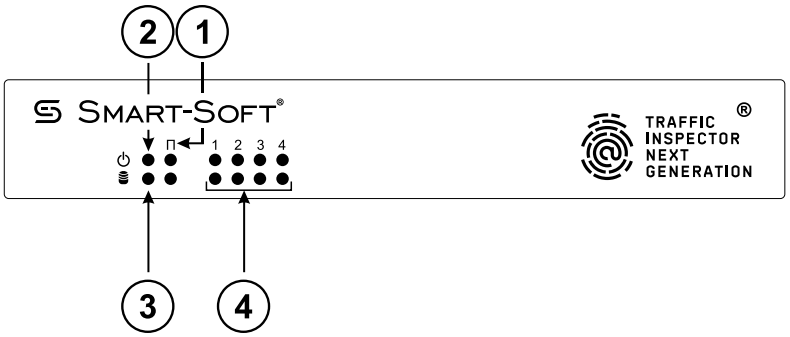
1. VGA D-SUB
2. USB
3. Кнопка вкл./выкл.
4. Консольный порт RS-232
5. RJ12
6. Питание 12В

Аппаратное обеспечение

СЕРИЯ S100

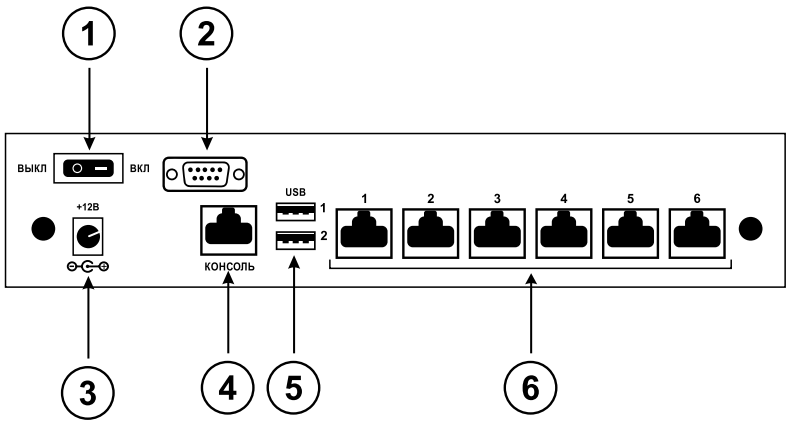
DEPO Stream 1060CX

Вид лицевой панели



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

Вид со стороны интерфейсов



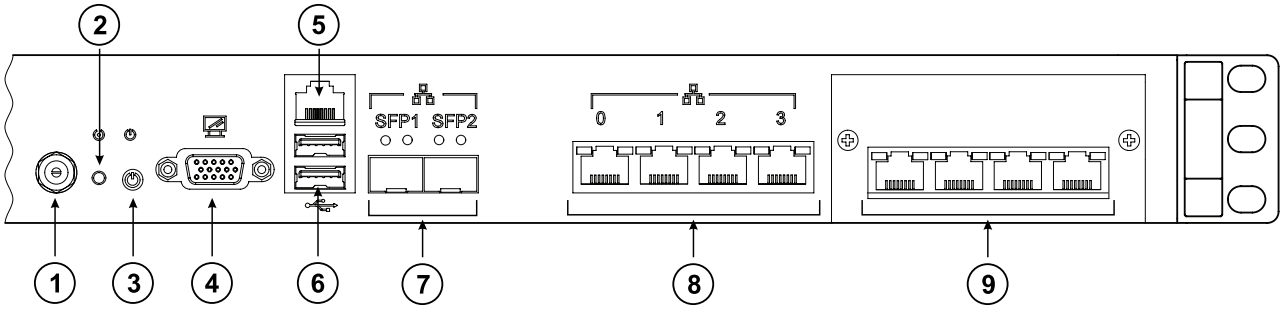
1. Кнопка включения
2. Порт D-Sub (VGA)
3. Разъем для подключения внешнего блока питания (PS)
4. Консольный порт RS-232
5. USB порты (2 шт.)
6. Сетевые порты RJ-45 ports

Аппаратное обеспечение

СЕРИЯ S300

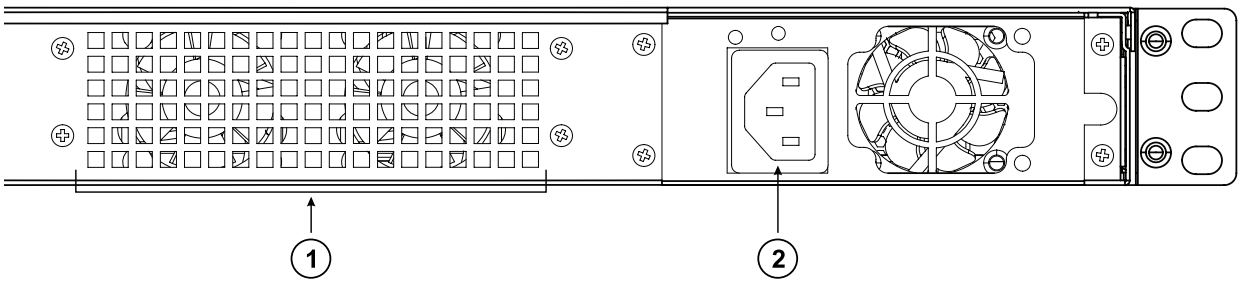
Аквариус T30 S001DC

Вид лицевой панели



1. Разъем электропитания DC In
2. Кнопка активации перезагрузки
3. Кнопка вкл/откл питания сервера с индикатором
4. Разъем VGA
5. Разъем последовательного порта Serial
6. Разъемы USB 3.0
7. Разъемы с индикацией для подключения SFP-модулей
8. LAN интерфейсы 1000BASE-TX
9. Интерфейсы сетевого модуля

Вид со стороны интерфейсов

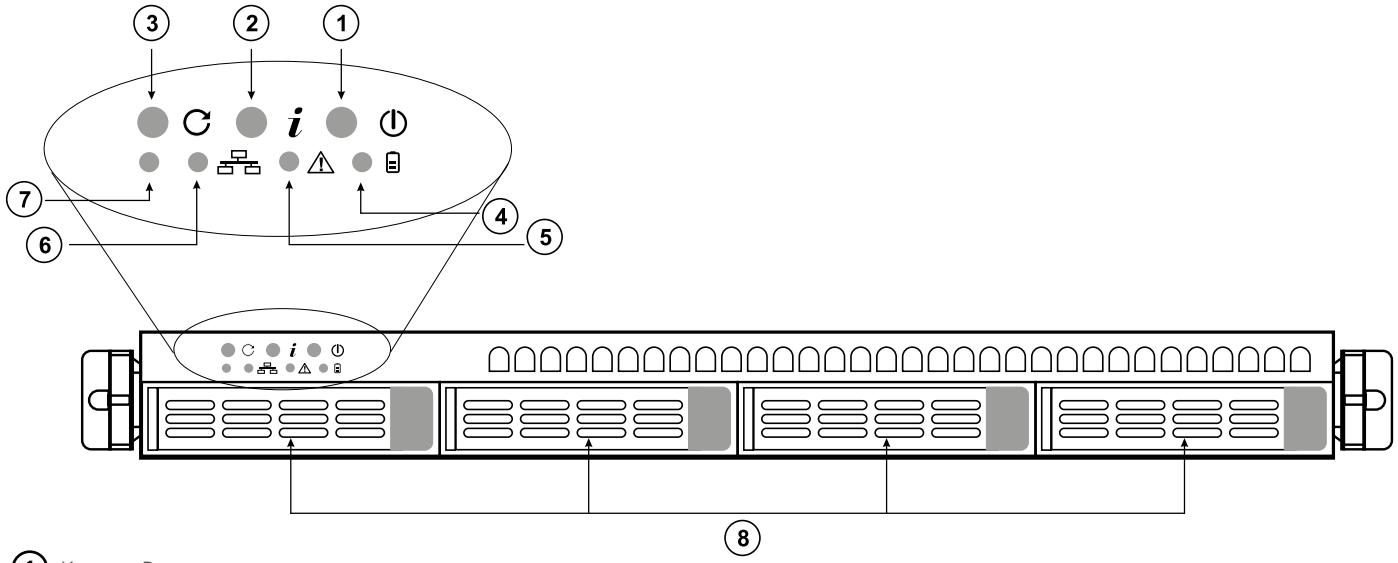


1. Вентиляционные отверстия
2. Разъем питания

СЕРИИ S500, M1000, L1000+

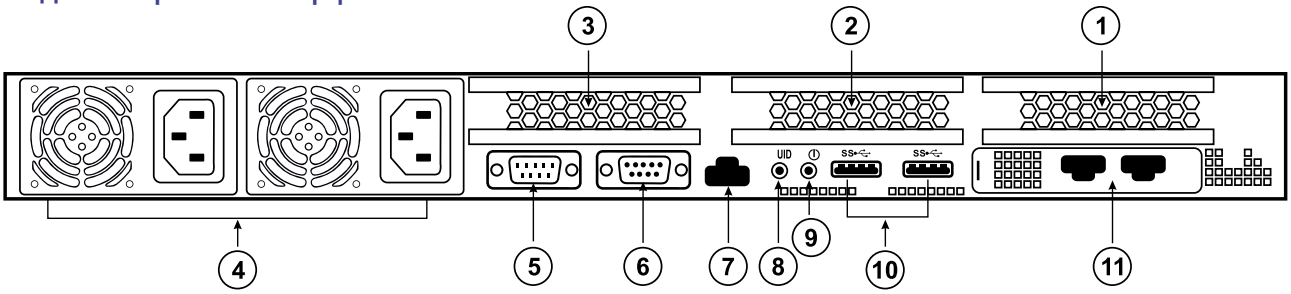
DEPO Storm 3450A1, DEPO Storm 3470Z1A

Вид лицевой панели



1. Кнопка Power с индикатором
2. Кнопка UID с индикатором
3. Кнопка Reset
4. Индикатор активности накопителей
5. Индикатор ошибки системы
6. Индикатор сети (не активен при отсутствии интегрированного LAN)
7. Индикатор активности выделенного порта управления
8. Лотки для накоптелей

Вид со стороны интерфейсов



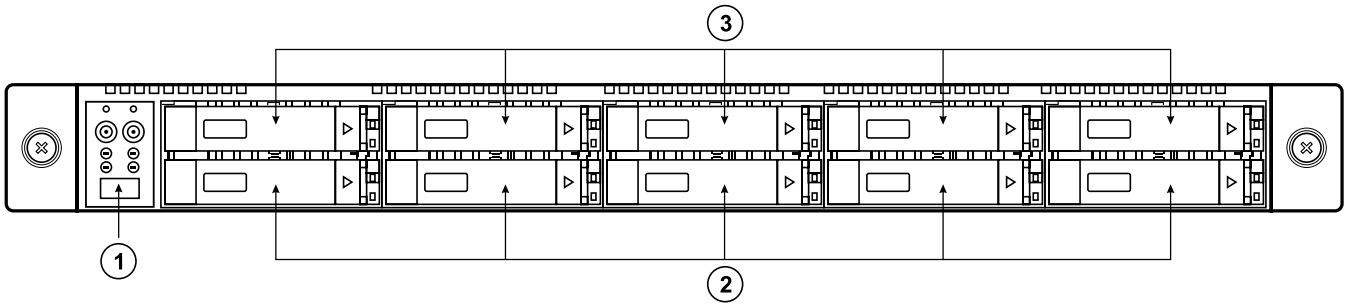
1. Слот расширения #1 x8/x16 (CPU1)
2. Слот расширения #2 x8 (CPU2)
3. Слот расширения #3 x8 (CPU1)
4. Блок питания с модулями 550Вт или 800Вт (опционально)
5. COM-порт
6. VGA-порт
7. Выделенный порт управления RJ-45
8. Кнопка UID
9. Кнопка Power
10. Порт USB 3.0
11. OCP 2.0 A Type слот (2xGbE или 2x10 GbE SFP+)

Аппаратное обеспечение

СЕРИЯ M700

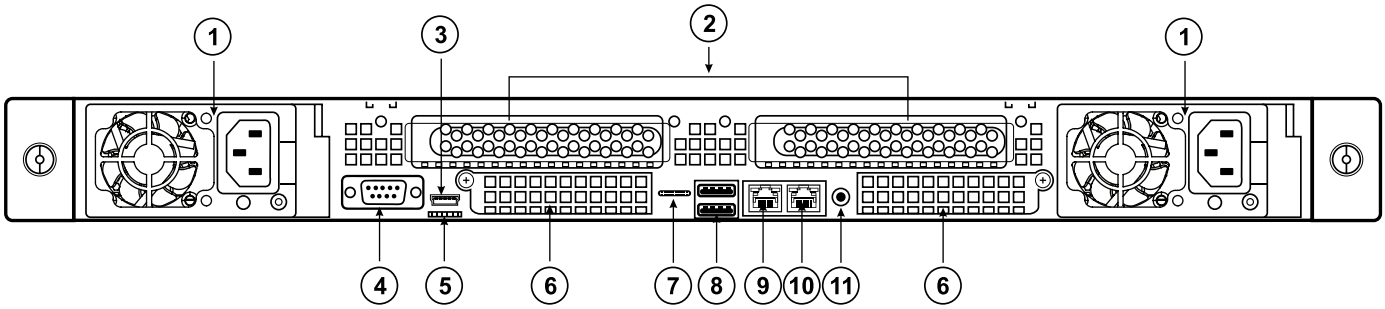
Аквариус T50 D110CF

Вид лицевой панели



1. Панель управления
2. Лотки для накопителей
3. Лотки для накопителей

Вид со стороны интерфейсов



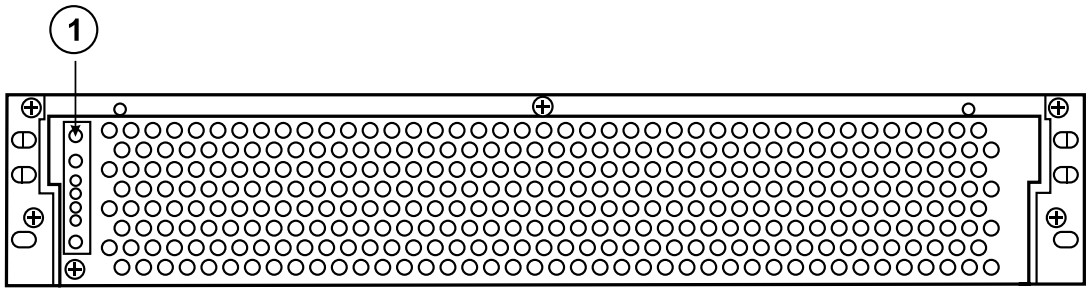
1. Блок питания (PSU)
2. Слоты расширения PCI
3. Serial port (mini USB type B)
4. VGA порт
5. Micro SD
6. Слот расширения OCP
7. USB 3.0 type C
8. 2xUSB 3.0
9. LAN1
10. Mgmt LAN
11. Кнопка с индикатором UID

Аппаратное обеспечение

СЕРИЯ L1500+

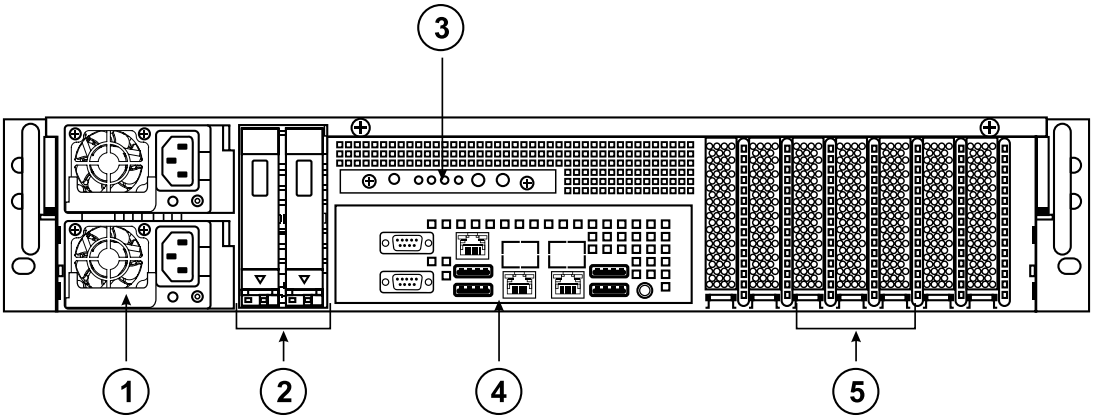
Аквариус T50 D202FW

Вид лицевой панели



1 Панель индикации

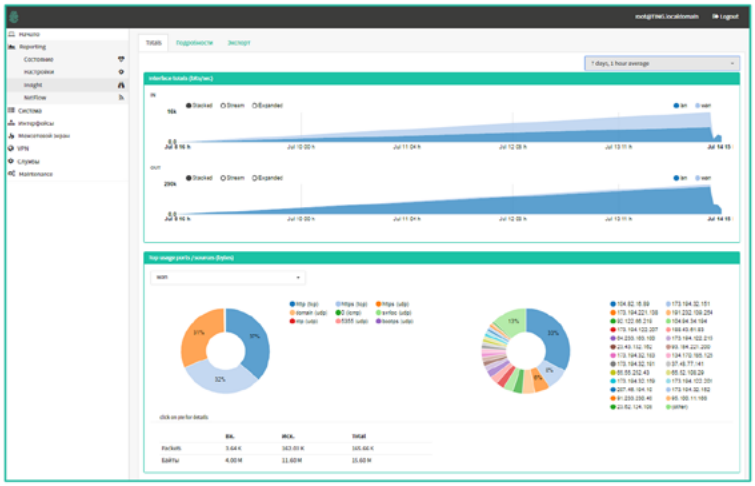
Вид со стороны интерфейсов



1. Блоки питания PSU1 и PSU2
2. Дисковые отсеки 2,5”, 2 шт
3. Панель индикации
4. Панель ввода/вывода
5. Слоты расширения PCI, 4 шт

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 или IPsec 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 1.13 на базе OPNsense 24.1 и FreeBSD 13.2)*

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

- Национальный удостоверяющий центр Минцифры России
- 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
- Поддержка в режиме прозрачного проксирования http- и https-траффика протокола WCCP2, предназначенного для перенаправления трафика в реальном времени
- 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
- Сохранение снимков состояния системы с возможностью отката на любой из них (при установке на ZFS)

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 переустановки пакета
- Запрет на обновление конкретного пакета
- Возможность аудита
  - Проверка установленных пакетов на наличие уязвимостей
- Поддержка плагинов

Интерфейс программирования REST
- Внешнее управление с помощью доверенного стороннего ПО
- Автоматизация обмена данными в реальном времени

Central Management System
- Централизованная панель управления несколькими узлами на головном узле
- Возможность использования внешнего центра сертификации (certification authority, CA) для установления доверительных отношений главным узлом и подчинёнными
- Синхронизация отдельных правил и конфигураций для пользовательских и групповых списков управления доступом (Access Control List, ACL) в прокси-сервере

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 1.10.2.F_58) **

- Аудит контрольных сумм файлов базовой системы, ядра и пакетов ПО
- Защита от несанкционированных изменений конфигурации системы
- Отключены встроенные антивирусы
- Отсутствует сканер безопасности сети
- Отсутствует web сервер nginx
- Отсутствует web application firewall
- Отсутствует обратный прокси на базе плагина nginx

** **Примечание:** функциональные возможности ФСТЭК-версии ограничены по сравнению с перечнем функциональных возможностей версии 1.12.0. Уточняйте состав функций ФСТЭК-версии у работников отдела продаж (sales@smart-soft.ru).

Семейство Traffic Inspector Next Generation

Программно-аппаратные комплексы

Производители АП:
DEPO, AQUARIUS, New Platforms



Программное обеспечение

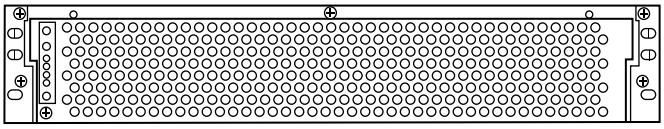
От 5 учетных записей

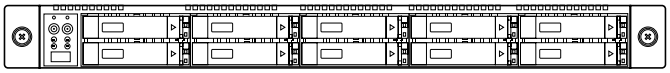


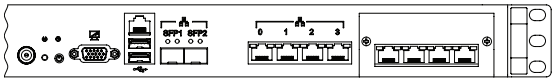
Семейство Traffic Inspector Next Generation FSTEC

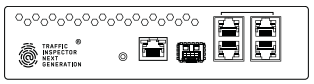
Программно-аппаратные комплексы

Производители АП:
AQUARIUS, New Platforms









Малые сети
S100 FSTEC-NP

Средние сети
S300 FSTEC-AQ

Крупные корпоративные сети
M700 FSTEC-AQ

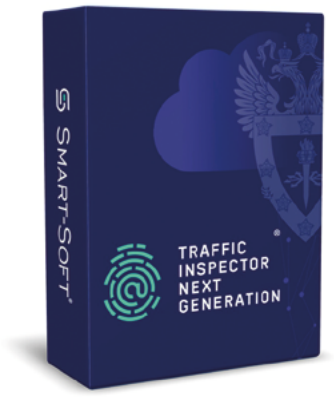
Масштабируемые корпоративные сети
L1500 FSTEC-AQ

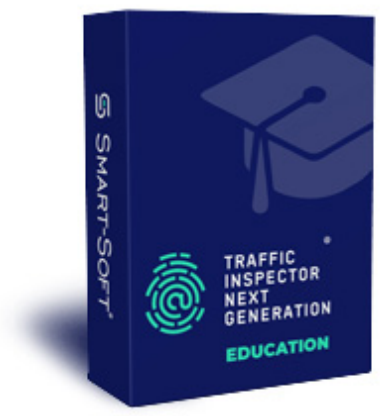
Размер корпоративной сети

Программное обеспечение

От 5 учетных записей







Технические характеристики аппаратных платформ Traffic Inspector Next Generation

Наименование	Характеристики	Производитель
Traffic Inspector Next Generation S100-NP **Traffic Inspector Next Generation S100 FSTEC-NP**	NP-1002i CPU C3538 (4 core) / RAM 16 Gb / 512 Gb / без VGA	New Platforms
Traffic Inspector Next Generation S100-DE	DEPO Stream 1060CX Intel® Celeron® N3060/ 8GB/ 1 x CF, 1 x SSD / HDD/ консольный порт Cisco-type RJ-45/ 6 сетевых портов Ethernet 1 Гбит/с (i211)	DEPO
Traffic Inspector Next Generation S300-AQ **Traffic Inspector Next Generation S300 FSTEC-AQ**	Аквариус T30 S001DC CPU Intel Atom C3758 2.2GHz, 8C/8T, 16MB, 25W/ CPU cooler/ RAM DIMM DDR4 16GB 2666MHz ECC/ SSD SATA 480GB 2.5" 7mm RI/ трансивер 1000BASE-T RJ-45 Copper SFP Optical Transceiver/ PSU 2x200W Hot-Swap, 80Plus/ кабель питания C13-C14, 1.8m	AQUARIUS
Traffic Inspector Next Generation S500-DE	DEPO Storm 3450A1 2xS4214/64GBRE2/SATA/2T1000G7/4HSA/4FN/ДАЦН.469535.001/2LAN1Ge/16D/1E/4GLAN/IPMI+/650W2HS/PCIe/RMK/CAR1S	DEPO
Traffic Inspector Next Generation M700-AQ **Traffic Inspector Next Generation M700 FSTEC-AQ**	Аквариус T50 D110CF CPU Intel Xeon Silver 4216 2.1GHz, 16C/32T, 22MB, 100W/ CPU cooler/ RAM RDIMM DDR4 16GB 3200MHz ECC/ SSD SATA 960GB 2.5" 7mm RI/ кабель HDminiSAS, SFF8643 - SFF8643, 0.7m/ кабель HDminiSAS, SFF8643 - SFF8643, 0.8m/ NIC PHY OCP mezz 10GbE, Dual port, 2xSFP+/ NIC PCI-E x4, 1GbE, Quad port, 4xRJ-45, HHHL (Intel i350)/ PSU 550W Hot-Swap, 80Plus Platinum, CRPS/кабель питания C13-C14, 3m	AQUARIUS
Traffic Inspector Next Generation M1000-DE	DEPO Storm 3470Z1A 2 x S4316 (2.3 GHz, 20 ядер, 25+30Mb, 150W, 10.4 GT/s LGA4189)/ 64GB/ SATA RAID 0/1/5/10/ NVMe NVME RAID Key/ BMC поддерживает IPMI, SOL, KVM Over IP, virtual media/ 6x RJ-45 (на базе Intel i350)/ 4x SFP (на базе Intel i350)/ 2x SFP+ (на базе Intel 82599ES или X710)	DEPO
Traffic Inspector Next Generation L1000+-DE	DEPO Storm 3470Z1A 2 x S4316 (2.3 GHz, 20 ядер, 25+30Mb, 150W, 10.4 GT/s LGA4189)/ 128 GB (4 x 32 ГБ DDR4 ECC REG)/ 12x SATA-III + 2x SATA III/ 3 x 2000 ГБ SATA-накопитель (7200 об/мин)/ DP, C621A, 32DIMM, 12xSATA3, 3 PCIE 4.0 x16, 2RSC, 2x10GB LAN (SFP), 2USB, VGA, COM (3.5" Jack), выделенный порт управления RJ-45/ 4x RJ-45 (1 Гбит/с), 2x SFP (10 Гбит/с)	DEPO
Traffic Inspector Next Generation L1500+-AQ **Traffic Inspector Next Generation L1500 FSTEC-AQ**	Аквариус T50 D202FW CPU Intel Xeon Gold 5218R 2.1GHz, 20C/40T, 27.5MB, 125W/ CPU cooler/ RAM RDIMM DDR4 32GB 3200MHz ECC/ SSD SATA 960GB 2.5" 7mm RI/ кабель HDminiSAS - 4xSATA, SFF8643 - 4xSATA, 0.8-1m для серверов CF/FW/BJ/ NIC PCI-E x8, 10GbE, Quad port, 4xSFP+, HHHL (Intel X710)/ NIC PCI-E x8, 40GbE, Dual port, 2xQSFP+ (Intel XL710)/ PSU 800W Hot-Swap, 80Plus Platinum, reversed airflow, CRPS/ кабель питания C13-C14, 1.8m	AQUARIUS

Бесплатное тестирование

Выбор решения по обеспечению информационной безопасности — ответственный процесс, требующий серьезного подхода. Как правило, компания-заказчик составляет перечень требований к решению в форме технического задания, в соответствии с которым выбирает оптимальный по параметрам продукт.

Самый надежный способ убедиться в том, что выбранный вариант решит поставленные задачи — проверить его в боевых условиях, протестировать работу всех необходимых функций.

Понимая потребности клиентов, «Смарт-Софт» предлагает в течение **30 дней бесплатно** протестировать Traffic Inspector Next Generation.

Свяжитесь с нами по почте **info@smart-soft.ru** или телефону **+7 (495) 775-59-91.**



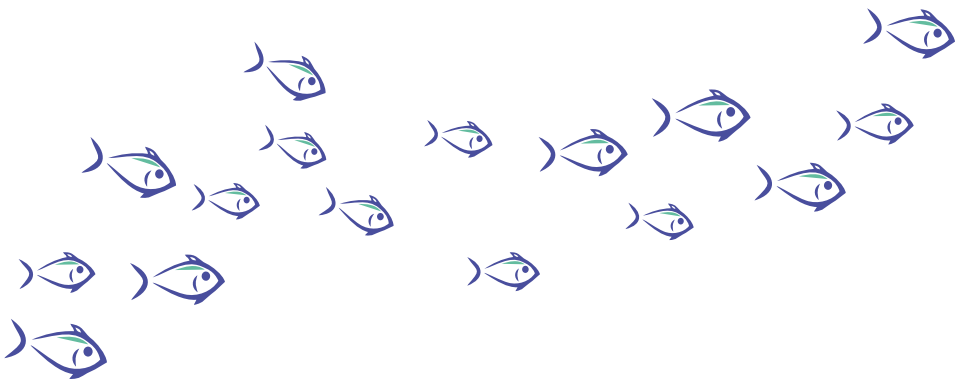
Миграция на Traffic Inspector Next Generation

Для пользователей многофункционального межсетевого экрана Traffic Inspector, а также для пользователей USG, UTM и NGFW других производителей действует скидка **30%** на программное обеспечение Traffic Inspector Next Generation (кроме Traffic Inspector Next Generation SaaS).

Скидка предоставляется при переходе на Traffic Inspector Next Generation с таким же количеством пользователей, как у продукта другого производителя, в соответствии с данными лицензионного соглашения.

Чтобы узнать подробности, свяжитесь с нами по почте **info@smart-soft.ru** или телефону **+7 (495) 775-59-91**.

Практический кейс мягкой миграции с ForiGate на Traffic Inspector Next Generation



Особые условия покупки Traffic Inspector Next Generation для образовательных учреждений и НКО

Смарт-Софт предоставляет особые условия покупки для следующих организаций:

- Российские учреждения образования: дошкольные, общеобразовательные, профессиональные, высшего образования, дополнительного профессионального образования.
- Российские некоммерческие организации и благотворительные фонды (исключая политические партии, религиозные организации, жилищно-строительные кооперативы, адвокатские образования).

Заказчики из сферы образования и НКО могут приобретать как базовую, так и сертифицированную ФСТЭК версию программного обеспечения Traffic Inspector Next Generation по цене на **15%** ниже текущей стоимости соответствующей базовой лицензии.

Для получения скидки организация, относящаяся к перечню льготных категорий, должна подтвердить свой статус, предоставив в Смарт-Софт документы, удостоверяющие ее сферу деятельности и организационно-правовую форму.

Чтобы узнать подробности, свяжитесь с нами по почте **info@smart-soft.ru** или телефону **+7 (495) 775-59-91**.



Смарт-Софт — российский разработчик решений в области информационной безопасности, работающий с 2003 года. Компания создает комплексные системы защиты корпоративных сетей от кибератак, реализуя стратегию многоуровневой (эшелонированной) обороны ИТ-инфраструктуры заказчиков.

Флагманские продукты:

- Traffic Inspector Next Generation (TING) — межсетевой экран следующего поколения (NGFW) с функциями фильтрации трафика, предотвращения угроз и контроля доступа.
- Traffic Inspector — универсальное решение для базовой и продвинутой защиты сетей, подходящее для малого и среднего бизнеса.

Продукты компании включены в Единый реестр российского ПО Минцифры и сертифицированы ФСТЭК России, что обеспечивает их использование в госсекторе и организациях с повышенными требованиями к безопасности.

Ключевая философия: адаптация защиты под специфику бизнеса клиентов — от отраслевых особенностей до масштаба инфраструктуры. Смарт-Софт делает ставку на импортозамещение, предлагая конкурентоспособные аналоги зарубежным решениям, и расширяет партнёрскую сеть для работы с государственными учреждениями, корпорациями и телеком-сектором.

5 фактов о компании Смарт-Софт

Российский разработчик
Разработка и техническая поддержка продуктов в России.

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

3 000 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.

© 2003-2025, СМАРТ-СОФТ