



С-ТЕРРА

Виртуальный Шлюз

Программный комплекс, предназначенный для защиты сетевого трафика, проходящего между различными компонентами виртуальных сред.

Работает в наиболее популярных гипервизорах (VMware ESXi, Citrix XenServer, KVM, Microsoft Hyper-V, Huawei Fusion).

ПРЕИМУЩЕСТВА

- Переход к полностью виртуальной инфраструктуре внутри компании
- Полная функциональность VPN-устройства С-Терра Шлюз
- Быстрая доставка, установка и настройка
- Высокая производительность шифрования трафика
- Эффективное использование ресурсов
- Оперативная адаптация к меняющимся задачам и требованиям сетевых приложений и инфраструктуры
- Легкое сохранение и восстановление резервной копии

ПРИМЕНЕНИЕ

Защита периметра виртуальной среды	Надежная защита корпоративной информации, безопасный информационный обмен между различными ЛВС организации осуществляются в полном соответствии с требованиями регуляторов.
Защита сетевых взаимодействий внутри виртуальной среды	Межсетевое экранирование и шифрование данных обеспечивает разграничение зон с разным уровнем доверия или выделение нескольких доменов безопасности внутри виртуальной среды.
Безопасный удаленный доступ к виртуальной среде	Работа с удаленными виртуализированными сервисами, независимо от расстояний и часовых поясов, настолько же безопасна, как и при локальном доступе.
Защита физических каналов связи между элементами виртуальной среды	Рекордная производительность позволяет защитить связь географически удаленных компонентов одной виртуальной сети (например, основной и резервный ЦОД), гарантируя конфиденциальность передаваемых данных.
Недорогое сертифицированное решение для малого и среднего бизнеса	Гибкое и легко масштабируемое решение, позволяющее эффективно использовать вычислительные ресурсы, оптимизировать энергопотребление и затраты, идеально подходит для динамично развивающегося бизнеса.
VPN-как-сервис для подключения к облачным ИС	Простое и экономически эффективное решение легко и быстро интегрируется в существующую инфраструктуру корпоративной сети.

ХАРАКТЕРИСТИКИ

- Шифрование и имитозащита трафика по протоколам IPsec ESP
- Аутентификация устройств по протоколу IKE
- Интегрированный межсетевой экран
- Пакетная фильтрация трафика
- Инкапсуляция IPsec трафика на основе протокола HTTP
- Обработка открытого и шифрованного трафика, в т.ч. split tunneling
- Туннелирование трафика
- Приоритизация и маркировка трафика (QoS)
- Интеграция с Radius сервером
- Событийное протоколирование Syslog, мониторинг SNMP
- Построение отказоустойчивых схем

<p>ПРОИЗВОДИТЕЛЬНОСТЬ</p>  <p>зависит от серверной аппаратной платформы (до 350 Мбит/с на 1 ядро процессора)</p>	<p>ГИПЕРВИЗОРЫ</p>  <p>VMware ESXi, Citrix XenServer, KVM, Microsoft Hyper-V, Huawei Fusion</p>
<p>СЕРТИФИКАЦИЯ</p>  <p>ФСБ России: КС1 ФСТЭК России: МЭ Б4, НДВ 4, ОУД 3</p>	<p>КРИПТОГРАФИЧЕСКИЕ БИБЛИОТЕКИ</p>  <p>C-Terra ST</p>

s•terra®

+7 (499) 940 9001

sales@s-terra.ru, www.s-terra.ru