



КОД
безопасности

КОНТИНЕНТ TLS

Система обеспечения защищенного удаленного доступа к веб-приложениям с использованием алгоритмов шифрования ГОСТ

ПРЕИМУЩЕСТВА



ТУННЕЛИРОВАНИЕ TSP-ТРАФИКА
ЧЕРЕЗ ПРОТОКОЛ TLS



УПРАВЛЕНИЕ И МОНИТОРИНГ
ОСУЩЕСТВЛЯЮТСЯ ЧЕРЕЗ ВЕБ-ИНТЕРФЕЙС,
ДОСТУПНЫЙ ИЗ ЛЮБОГО БРАУЗЕРА



НЕОГРАНИЧЕННАЯ МАСШТАБИРУЕМОСТЬ
ПРИ ИСПОЛЬЗОВАНИИ ВНЕШНЕГО
БАЛАНСИРОВЩИКА



ЛИЦЕНЗИРОВАНИЕ ПО ОДНОВРЕМЕННОМУ,
А НЕ ОБЩЕМУ КОЛИЧЕСТВУ УДАЛЕННЫХ
ПОЛЬЗОВАТЕЛЕЙ



ИСПОЛНЕНИЕ В ВИДЕ ОТДЕЛЬНОГО
УСТРОЙСТВА



СИСТЕМА РАЗГРАНИЧЕНИЯ ПРАВ
УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ
ПОРТАЛА ПРИЛОЖЕНИЙ



ИНТЕГРАЦИЯ С ACTIVE DIRECTORY,
SIEM-СИСТЕМАМИ И WAF



ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ – ДО
45 000 ОДНОВРЕМЕННЫХ ПОДКЛЮЧЕНИЙ



ШИФРОВАНИЕ

- Криптографическая защита HTTPS-трафика по протоколу TLS
- Поддерживаемые криптоалгоритмы:
 - Шифрование информации производится по алгоритму ГОСТ 28147–89
 - Расчет хэш-функции по алгоритму ГОСТ Р 34.11–2012
 - Формирование и проверка электронной подписи осуществляются в соответствии с алгоритмом ГОСТ Р 34.10–2012
- Поддерживаемые протоколы:
 - TLS v1.0
 - TLS v1.2
- Возможность работы с различным клиентским ПО:
 - «Континент TLS Клиент»
 - Поддержка туннелирования TCP-трафика через протокол TLS
 - Поддержка работы пользователя в любом браузере
 - «КриптоПро CSP»
 - Работа пользователя в браузере Internet Explorer
 - Валидата CSP
 - Браузер «Спутник»
 - Яндекс.Браузер
 - Любой другой клиент, соблюдающий спецификацию TLS

СЕТЕВЫЕ ВОЗМОЖНОСТИ

- Скрытие защищаемых серверов (обратный прокси-сервер)
 - К каждой сессии пользователя может быть добавлен произвольный идентификатор
- Работа в режиме кластера с балансировкой нагрузки
 - Неограниченное линейное масштабирование производительности
- Блокировка неиспользуемых портов

КОНТРОЛЬ ДОСТУПА К ЗАЩИЩАЕМЫМ РЕСУРСАМ

- Идентификация и аутентификация пользователей по сертификатам открытых ключей стандарта x.509v3 (ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012)
- Обоюдная аутентификация пользователя и сервера в процессе установки защищенного соединения
- Проверка сертификатов ключей по спискам отозванных сертификатов (CRL)
- Автоматическая загрузка и обновление Trust-service Status List (TSL)
- Интеграция с Active Directory при работе сервера удаленного доступа в режиме портала приложений:
 - Аутентификация пользователя по имени пользователя и паролю AD
 - Предоставление доступа к приложениям на основе принадлежности пользователя к структурному подразделению
- Аутентификация с учетом значений различных полей
- NTLM аутентификация для ресурсов
- Single-Sign-On в приложениях портала
- Интеграция с сервисом auth.as.

РЕЖИМЫ РАБОТЫ

- Шифрование HTTP/HTTPS-трафика
- Туннелирование произвольного TCP-трафика через протокол TLS
- Публикация приложений на портале

УПРАВЛЕНИЕ И МОНИТОРИНГ

- Веб-интерфейс для управления и мониторинга
- Интеграция в SIEM-систему по протоколу syslog
- Регистрация событий информационной безопасности, связанных с работой «Континент TLS Клиент»

СЦЕНАРИИ ПРИМЕНЕНИЯ

ВЫСОКОНАГРУЖЕННЫЙ ПОРТАЛ ГОСУДАРСТВЕННЫХ УСЛУГ

Результат:

- Минимизированы затраты на построение и эксплуатацию комплексной системы защищенного доступа к portalу государственных услуг.
- Повышена производительность приложения за счет переноса подсистемы шифрования трафика на отдельное устройство.

СИСТЕМА УДАЛЕННОГО ДОСТУПА К РЕСУРСАМ ПРЕДПРИЯТИЯ

Результат:

- Организован доступ удаленных пользователей к внутренним веб-приложениям
- Обеспечено разграничение доступа удаленных пользователей к различным веб-приложениям
- Обеспечен доступ пользователей к корпоративным ресурсам с помощью толстых программных клиентов (терминалов, клиентов ERP-систем и т.д.)







СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Результат:

- Информационная система приведена в соответствие требованиям приказа ФСТЭК России № 17 (ИАФ, УПД, ЗИС, РСБ, ОЦЛ, ОДТ, ЗТС)
- Минимизированы затраты на встраивание сертифицированной криптографии в приложения, к которым осуществляется удаленный доступ
- Минимизированы риски, связанные с невыполнением требований регуляторов

МОДЕЛЬНЫЙ РЯД

МОДЕЛЬ	IPC-50	IPC-500	IPC-1000	IPC-3000
				
Форм-фактор	Mini-ITX	1U rack	1U rack	1U rack
Производительность в режиме HTTPS-прокси, Мбит/с	до 890 Мбит/с	до 890 Мбит/с	до 890 Мбит/с	до 4 000 Мбит/с
Количество одновременных подключений	до 4 000	до 10 000	до 10 000	до 45 000
Интерфейсы RJ-45 (медь UTP)	4x 1000BASE-T Ethernet 10/100/1000	6x 1000BASE-T Ethernet 10/100/1000	8x 1000BASE-T Ethernet 10/100/1000	1x 1000BASE-T Ethernet 10/100/1000
Интерфейсы оптические	1x 1000BASE-X Ethernet SFP	—	8x 1000BASE-X Ethernet SFP	4x 10 Gigabit Ethernet SFP+

СЕРТИФИКАТЫ



ФСБ России

ПАК «Континент TLS Сервер»: СКЗИ КС2

ФСТЭК России

4 уровень контроля отсутствия НДВ

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.

В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Существует несколько пакетов технической поддержки:



Базовый



Стандартный



Расширенный



VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный)

info@securitycode.ru

www.securitycode.ru