CITIC TELECOM CPC

TrustCSI™ Унифицированное управление угрозами UTM

Унифицированное управление угрозами. Ваше управляемое решение сетевой безопасности с интеллектуальной комплексной системой оповещений

Открытость Интернета, разносторонность современных предприятий и разветвленные связи между внутренней и внешней средой представляют собой риски взломов, угроз и уязвимостей как извне, так и изнутри.

Многие предприятия пользуются брандмауэрами и виртуальными частными сетями в качестве обороны первого эшелона против зловредного трафика, что может обеспечить лишь минимальную защиту от известных угроз, но оставляет сеть незащищенной от возникающих непреднамеренных угроз со стороны сотрудников самих компаний.

Чтобы гарантировать полную защиту информации организаций, компания CITIC Telecom CPC представила решение для первого эшелона защиты **TrustCSI™ UTM** , не требующее капитальных затрат и комплексной технической поддержки.

ОСНОВНЫЕ ОСОБЕННОСТИ

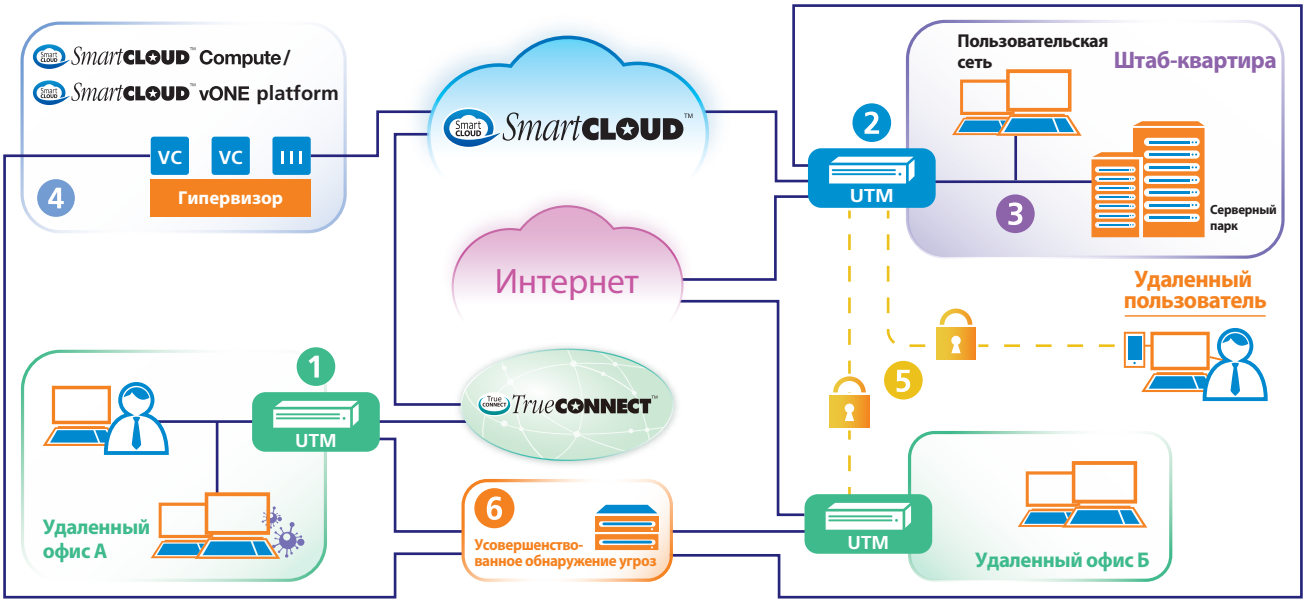
- Полностью управляемое экспертами безопасности решение с круглосуточным мониторингом в режиме реального времени, поддержкой на местах и «горячей линией», единым оповещением и платформой сопоставления данных журналов SIEM
- Комплексное решение с брандмауэром, антивирусом, системами IPS и контроля активности в Интернете
- Веб-портал для конечных пользователей, работающий в режиме реального времени, и еженедельная отчетность
- Опциональная система TrustCSI™ UTM NFV обеспечивает 99,99%-ную доступность сервиса с одним виртуальным модулем, поддерживаемым инфраструктурой SmartCLOUD™
- Гибкая ежемесячная оплата, модернизация и масштабирование по потребностям бизнеса
- Управление конфигурацией устройств, резервирование данных и замена аппаратной части
- Дополнительные опции, в том числе IPSec VPN и SSL VPN
- Дополнительный виртуальный модуль TrustCSI™ UTM NFV сокращает время обслуживания клиентов SmartCLOUD™ по сравнению с традиционными UTM на аппаратной основе

Надежный партнер в сфере информационно-коммуникационных технологий

中信國際電訊(信息技術)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED | *Представитель* CITIC TELECOM INTERNATIONAL

TrustCSI™ UTM Unified Threat Management

Всесторонний подход к корпоративной сети



1. Защита от перекрестного заражения на уровне MPLS с функцией аутентификации пользователей

Согласно схеме, решение TrustCSI™ UTM может предотвратить внутренние угрозы в корпоративной MPLS-сети путем блокировки вируса в удаленном офисе A и препятствия его передачи в другие удаленные офисы, т. е. удаленный офис Б и штаб-квартиру. Функция аутентификации пользователей обеспечивает еще больший уровень контроля доступа к критическим приложениям. Доступ будет предоставлен только пользователям с необходимой аутентификацией, такой как "e-cert", т. е. пользователю B на схеме.

2. Защита шлюза на уровне Интернета

Во избежание проникновения угроз в корпоративную сеть через Интернет во время его использования сотрудниками решение TrustCSI™ UTM может обеспечивать эффективную защиту передачи информации в незащищенной зоне Интернета с помощью передовых функций защиты.

3. Защита важных активов

Для защиты критически важных активов предприятий, которые более уязвимы к атакам с разрушительными последствиями, решение TrustCSI™ UTM может предложить различные модели развертывания, сегментирующие корпоративную сеть на отдельные зоны. Создается эффективная защита как от внутренних, так и внешних угроз, охватывающая в том числе и внутренние файловые серверы, к которым часто получают доступ сотрудники и серверы с выходом в Интернет.

4. Виртуализированный шлюз безопасности на SmartCLOUD™

Для полноценной реализации гибкости и преимуществ пакета на основе виртуальной машины решение TrustCSI™ UTM можно развернуть в этой форме (виртуальной машины) для защиты инфраструктуры предприятия на платформе SmartCLOUD™ Compute или vONE. Обеспечивается быстрое развертывание и высокая отказоустойчивость.

5. Гибкое развертывание частной виртуальной сети для защищенного удаленного доступа

Из схемы видно, что корпоративную сеть можно протянуть до удаленного офиса Б через Интернет с защищенным каналом IPSec поверх имеющегося интернет-соединения. Удаленные пользователи могут использовать мобильные устройства для доступа к внутренним ресурсам (файловые серверы, бизнес-приложения) по защищенным каналам SSL VPN.

6. Усовершенствованное обнаружение развитых устойчивых угроз

Для борьбы с развитыми устойчивыми угрозами (APT) решение TrustCSI™ UTM может быть совмещено с усовершенствованными средствами обнаружения угроз путем развертывания модуля безопасной (изолированной) среды или подписки на облачную тестовую среду. При обнаружении вредоносного или подозрительного файла модуль изолированной среды отправит уведомление системе UTM и автоматически примет защитные меры.

CITIC Telecom CPC

Сайт: www.citictel-cpc.com
Азиатско-тихоокеанский регион: info@citictel-cpc.com
Европа и СНГ: info-eu@citictel-cpc.com

Гонконг: 852 2170 7101
Япония: 81 3 5339 1968
Эстония: 372 622 33 99
Польша: 48 22 630 63 30
Тайвань: 886 2 6600 2588
Малайзия: 603 2280 1500
Латвия: 371 6721 4122
Россия: 7 495 657 9277
Континентальный Китай (бесплатный звонок): 400 880 1222
Сингапур: 65 6220 6606
Литва: 370 5264 4303
Нидерланды: 31 20 567 2000

STA1802EN