Ростех

Акционерное общество «Концерн «Автоматика»

масштаб
научно-
исследовательский
институт

Функциональные характеристики программного обеспечения ПК **КРОНОС**™

Характеристики	Подробные сведения
Межсетевой экран	
Преобразование сетевых адресов (NAT)	Поддержка статической/скрытой трансляции NAT с задаваемыми вручную и автоматически правилами
Настройка демилитаризованной зоны (DMZ)	Настройка DMZ в сочетании с маршрутизацией и трансляцией адресов (NAT) или трансляцией портов (PAT)
Пакетная фильтрация	Фильтрация IP-пакетов в соответствии с заданными правилами фильтрации на основе: — IP-адресов отправителя и получателя — сетевых интерфейсов — протоколов — номеров портов UDP/TCP — флагов TCP/IP-пакетов — времени — состояния соединений Фильтрация прикладных протоколов с использованием регулярных выражений Фильтрация трафика по мандатным меткам
Виртуальные частные сети	
Поддержка шифрования сети VPN на основе технологии IPSec	AES 128-256 бит, 3DES 56-168 бит
Туннелирование	PPPoE, IPIP, GRE, L2TP, PPTP, OpenVPN, MLPPP
Виртуальные локальные сети	
Построение виртуальных локальных сетей	Функционирование VLAN IEEE 802.1Q, поддержка технологии VXLAN в режиме «точка-точка»
Обнаружение вторжений и атак	
Защита на сетевом уровне	Блокирование атак типа: Dos, сканирование портов, атаки связанные с протоколами IP/ICMP/TCP
Пассивный мониторинг	Пассивный мониторинг протокола DNS, блокировка запросов на URL адреса
Выявление аномалий	Выявление аномалий сетевого трафика и сетевых атак
Интеграция с подсистемами мониторинга	Обеспечение интеграции с подсистемами мониторинга, управления и корреляции событий информационной безопасности по протоколу Syslog
Журналирование	Гибкость генерации отчетов
Управление и мониторинг	Централизованное управление и мониторинг посредством CLI, используя удаленное подключение по протоколу SSHv2
Сетевые возможности	
Поддержка динамической маршрутизации	RIPv2, OSPFv2, BGPv4, многоадресная передача
Поддержка DHCP	Распределение IP-адресов посредством DHCP тремя способами: — ручное распределение — автоматическое распределение — динамическое распределение Ретрансляция сообщений DHCP между клиентами и серверами в разных подсетях
Маршрутизация на основе задаваемых политик policy-routing	Возможность маршрутизации в зависимости от значения поля ToS (DSCP), длины IP пакета, входного интерфейса, возможность настройки маршрутизации выделенных абонентов/подсетей через определенный шлюз
Обеспечение надежности сетей	Возможность автоматического переключения на резервный канал (VRRP) Функция отказоустойчивого кластера в конфигурации Активный/Пассивный Возможность мониторинга состояния каналов Ethernet по протоколам TCP, ICMP Обеспечение перенаправления (зеркалирования) трафика
Многоадресная передача	Функционирование по протоколу групповой маршрутизации для IP сетей, обеспечивающего эффективный механизм доставки дейтаграмм для групп хостов без организации соединений - PIM SM. Функционирование по протоколу IGMPv2
Сетевые сервисы	DNS-клиент, DNS-proxy, NTP клиент/сервер
Обнаружение сетевых устройств	Функционирование по протоколу LLDP
Обнаружение переполнения очередей	Предупреждение перегрузок с поддержкой следующих механизмов: RED, ECN, GRED
Организация, обработка очередей	Механизм управления очередями предусматривающий поддержку следующих методов: CBQ, SFQ, FIFO, PQ, HTB, HFSC
Приоритетная обработка трафика	Классификация и приоритетная обработка пакетов по следующим критериям: — порту(TCP/UDP) отправителя — порту (TCP/UDP) получателя — IP-адресу отправителя — IP-адресу получателя — MAC-адресу отправителя — значению поля «Протокол» заголовка IP — значению поля «ToS» (TOS/DSCP) заголовка IP — длине пакетов — значению 3 битов в теге 802.1Q Ethernet -кадра — совокупности указанных критериев Маркировка IP-пакетов, предусматривающая обработку поля DSCP в заголовке IP-пакета со следующими возможностями: — сохранение имеющегося значения — маркировка DSCP — перемаркировка DSCP
Целостность	Автоматический и ручной контроль целостности программного обеспечения
Управление	
Конфигурирование посредством CLI	Возможность конфигурирования себя посредством CLI следующими способами: — локально (путем ввода с клавиатуры текстовых команд) — удаленно (при подключении по протоколу SSHv2 или Telnet)
Аутентификация, авторизация	Поддержка парольной аутентификации

Ростех

Акционерное общество «Концерн «Автоматика»

масштаб
научно-
исследовательский
институт

КРОНОС™

ПРОГРАММНЫЙ КОМПЛЕКС

ПРОГРАММНЫЙ КОМПЛЕКС МЕЖСЕТЕВОГО ЭКРАНА С ФУНКЦИЯМИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Широкие функциональные возможности

Постоянный мониторинг и обнаружение вторжений в режиме, близком к реальному времени

Сокращение расходов за счет возможности развертывания в виртуальной среде

Программный комплекс **Кронос™** - межсетевой экран нового поколения, предназначенный для надежной защиты периметра коммерческих ведомственных сетей связи, центров обработки данных от внешних угроз и вторжений.

Кронос™ осуществляет пакетную фильтрацию, преобразование сетевых адресов и настройку демилитаризованной зоны (DMZ), фильтрацию трафика с возможностями построения защищенных каналов связи VPN и обнаружения вторжений IDS (СОВ).

КЛЮЧЕВЫЕ ОСОБЕННОСТИ ПРОДУКТА

- Высокая производительность - от 1 до 5 млн пакетов/с*
- Поддержка режимов динамической маршрутизации (протоколы RIPv2, OSPFv2, BGPv4, многоадресная передача)
- Производительность в режиме межсетевого экранирования - не менее 256 ООО конкурирующих (контролируемых) TCP сессий*
- Работа в конвергентных сетях: данные, голос, видео
- Потоковая фильтрация L2-L4

СЕРТИФИКАТЫ

МО РФ: №4537 от 06.12.2019 по 06.12.2024, НДВ-2, МЭ-2А, СОВ-2 (ИТ.СОВ.С2.ПЗ), РДВ.

*В зависимости от производительности аппаратной платформы, настроек маршрутизации, условий фильтрации и приоритизации трафика.

По всем вопросам обращайтесь по телефону (812) 309-03-21

194100, Санкт-Петербург, ул. Кантемировская д. 5, лит. А, (812) 309-03-21, sales@mashtab.org
www.mashtab.org

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Кронос™ обеспечивает:

- Обнаружение вторжений - защиту компьютерных сетей от хакерских атак
- Защиту локальной сети от нежелательного трафика
- Защиту корпоративной сети от DoS-атак
- Защищенное подключение удаленных пользователей к корпоративной сети
- Создание отказоустойчивых кластерных решений
- Разделение доступа к сегментам корпоративной сети, выделение сегмента DMZ
- Обеспечение стабильности приоритетных соединений независимо от остальной нагрузки
- Объединение локальных сетей структурных подразделений и филиалов в единую защищенную корпоративную сеть

Межсетевой экран

Кронос™ позволяет обеспечить защиту периметра, как небольшой организации, так и распределенной сети предприятия и его филиалов, безопасность межсетевых соединений между структурными подразделениями и комплексную безопасность центра обработки данных (ЦОД).

Маршрутизация

Кронос™ обеспечивает динамическую маршрутизацию трафика по протоколам RIPv2, 0SPFv2, BGPv4, а также на основе определяемых администратором политик policy-routing. Предусмотрена возможность перенаправления (зеркалирования) трафика и возможность задать полосу пропускания в зависимости от приоритизации.

Защита внутренних сетей

Кронос™ обеспечивает надежную защиту компьютерных сетей, позволяя осуществлять пакетную фильтрацию, преобразование сетевых адресов и настройку демилитаризованной зоны (DMZ).

Система обнаружения вторжений

Система обнаружения вторжений **Кронос™** анализирует входящий трафик, выявляя аномалии и сигнализируя при обнаружении подозрительной активности. Специальный программный модуль в составе **Кронос™** позволяет управлять, редактировать и разрешать применение обновляемых наборов сигнатур и эвристических правил выявления атак. Обновление баз данных осуществляется дистанционно.

Создание защищенных каналов VPN

Поддержка шифрования сети VPN на основе технологии IPSec (AES 128 бит, 3DES 192 бит) позволяет создавать с помощью **Кронос™** защищенные соединения (туннели) между структурными подразделениями организации, включая локальные и территориально-распределенные сети. Используемые протоколы туннелирования: PPPoE, IPIP, GRE, L2TP, PPTP.

Разграничение доступа

Управление доступом осуществляется как на основе ролевой модели, так и по дискреционному методу.

Отказоустойчивость

Повышенная отказоустойчивость обеспечивается благодаря поддержке работы по протоколу VRRP. Доступен режим отказоустойчивого кластера в конфигурации активный/пассивный с сохранением состояния сессий при переходе на резерв.

194100, Санкт-Петербург, ул. Кантемировская д.5, лит.А, (812) 309-03-21, sales@mashtab.org
www.mashtab.org

Ростех

Акционерное общество «Концерн «Автоматика»

масштаб
научно-
исследовательский
институт

ПОЛНОСТЬЮ РОССИЙСКАЯ РАЗРАБОТКА

- Наличие исходных кодов и документации в России
- Локализованные в России инфраструктура разработки и сервисная поддержка
- Внесено в единый реестр российских программ для электронных вычислительных машин и баз данных
- Русскоязычная документация и техподдержка

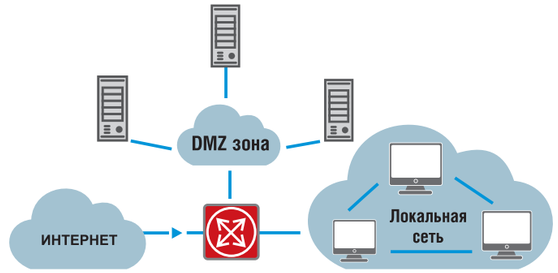
ВАРИАНТЫ ПРИМЕНЕНИЯ

Обеспечение безопасного доступа в Интернет

Кронос™ позволяет эффективно контролировать доступ в Интернет, обеспечивая учет трафика, протоколирование историю посещений, блокировку нежелательных ресурсов.

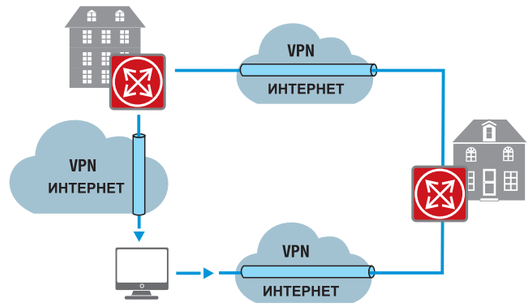
Защита внутренних сетей (DMZ)

Кронос™ позволяет защитить внутренние сети организации (веб-серверы, почтовые серверы, серверы баз данных и т. д.) от внешних и внутренних атак с помощью организации демилитаризованной зоны (DMZ). Это позволяет разрешить доступ определенным пользователям или группам, вести учет трафика, вводить ограничения.



Организация защищенного канала

Кронос™ легко позволяет установить защищенное соединение между распределенными подразделениями компании, а также организовать подключение удаленных пользователей с помощью VPN. В зависимости от мощности аппаратной платформы, на которую установлен **Кронос™**, можно обеспечить безопасность как небольшого подразделения, так и головного офиса крупной компании со штатом в несколько тысяч человек.



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Обеспечивается качественная гарантийная и сервисная поддержка продукта.

194100, Санкт-Петербург, ул. Кантемировская д.5, лит.А, (812) 309-03-21, sales@mashtab.org
www.mashtab.org