QazGate

Защити свою сеть с QAZGATE NGFW

QAZGATE NGFW - это комплексное решение для надежной, управляемой и защищенной работы в сети. Система соответствует 4-му уровню безопасности согласно СТ РК ISO/IEC 15408-3-2017F и входит в перечень программного обеспечения, которое соответствует требованиям информационной безопасности в госорганах.



QazGate

с 2018

защищаем сетевой периметр клиентов

50+

компаний работают с продуктами QAZGATE

100 000

отражаемых атак

100 млн

доменов и IP-адресов C&C в нашем BlockList

Ключевые преимущества Qazgate:

1. Продукт сертифицирован по 4-му уровню безопасности согласно СТ РК ISO/IEC 15408-3-2017F — это официальный уровень доверия, признанный в стране.

2. Поддержка национального стандарта СТ РК ISO/IEC 27002-2023, что упрощает соответствие ИБ-аудитам, проводимым НКБ РК, МЦРИАП, КНБ и другими контролирующими органами.

3. Интерфейс и документация доступны на казахском, русском и английском языках, что:
   Соответствует нормам закона «О языках»;
   Удобно для локальных администраторов и сотрудников ИБ;
   Отсутствие скрытых внешних зависимостей (в отличие от зарубежных NGFW)

Закон РК «О языках»

4. Стоимость лицензии фиксирована в тенге, без привязки к валютным колебаниям, что (Упрощает бюджетное планирование, защищает от девальвационных рисков, делает продукт доступным для региональных акиматов, ЦОНов, НПО и госшкол)

5. NGFW Qazgate - единственный продукт из класса Межсетевых экранов, входящий в реестр доверенного программного обеспечения и продукции электронной промышленности

Закон требования к организации информационной безопасности

ПРЕИМУЩЕСТВА NGFW QAZGATE ДЛЯ ГОСУДАРСТВА

QazGate



Укрепление цифрового суверенитета:

- Продукт разработан и сертифицирован в Казахстане, не содержит скрытых внешних зависимостей.
- Исключается риск внедрения «закладок» и внешнего управления через зарубежные NGFW.



Приоритет при госзакупках:

- Обоснование приоритета при закупках для нужд обороны, госслужб, МВД, КНБ и субъектов квазигоссектора.



Экономическая устойчивость:

- Облегчается бюджетное планирование на всех уровнях;
- Повышается доступность продукта для регионов, госшкол, ЦОНов и НПО
- Устраняется влияние валютных колебаний;



Развитие ИТ-сектора:

- Поддержка отечественного производителя усиливает:
- Занятость специалистов в ИТ;
- Технологическую независимость от зарубежных вендоров;
- Развитие локальной ИТ-инфраструктуры и компетенций.

ТЕНДЕНЦИЯ УРОВНЯ БЕЗОПАСНОСТИ В ШКОЛАХ РК

ШКОЛЬНИКИ СМОТРЕЛИ ПОРНО НА УРОКАХ В АЛМАТИНСКОЙ ОБЛАСТИ

НАСИЛИЕ В ШКОЛЕ: МНЕНИЯ ПСИХОЛОГОВ И ПУТИ РЕШЕНИЯ

ШКОЛАХ УСТЬ-КАМЕНОГОРСКА ДЕТИ СМОТРЕЛИ ПОРНО ВО ВРЕМЯ УРОКОВ

В ZOOM АКТЮБИНСКИЕ ШКОЛЬНИКИ ПОЛУЧАЮТ РАЗВРАТНЫЕ СООБЩЕНИЯ

QazGate

Власть над вашей сетью в ваших руках

QAZGATE NGFW — ваш инструмент для максимального контроля трафика. Повысьте производительность труда в компании.

Пожиратели времени (развлекательные и фейковые новости, соцсети, форумы, online-игры) крадут до 2-х часов рабочего времени сотрудника в день. Реклама и баннеры нарушают концентрацию внимания. Помогите коллегам сфокусироваться на рабочих процессах.



Блокируйте угрозы на дальних подступах и обезопасьте ваши данные и мощности

1

Защита от вирусов

95% вирусов попадают в локальную сеть из интернета. Более 80% зловредов загружают вредоносное содержимое из бот-сети и общаются с командными центрами (C&C). Заблокируйте их загрузку и узнайте о зараженных хостах, контролируя трафик на сетевом периметре.

2

Предотвращение атак

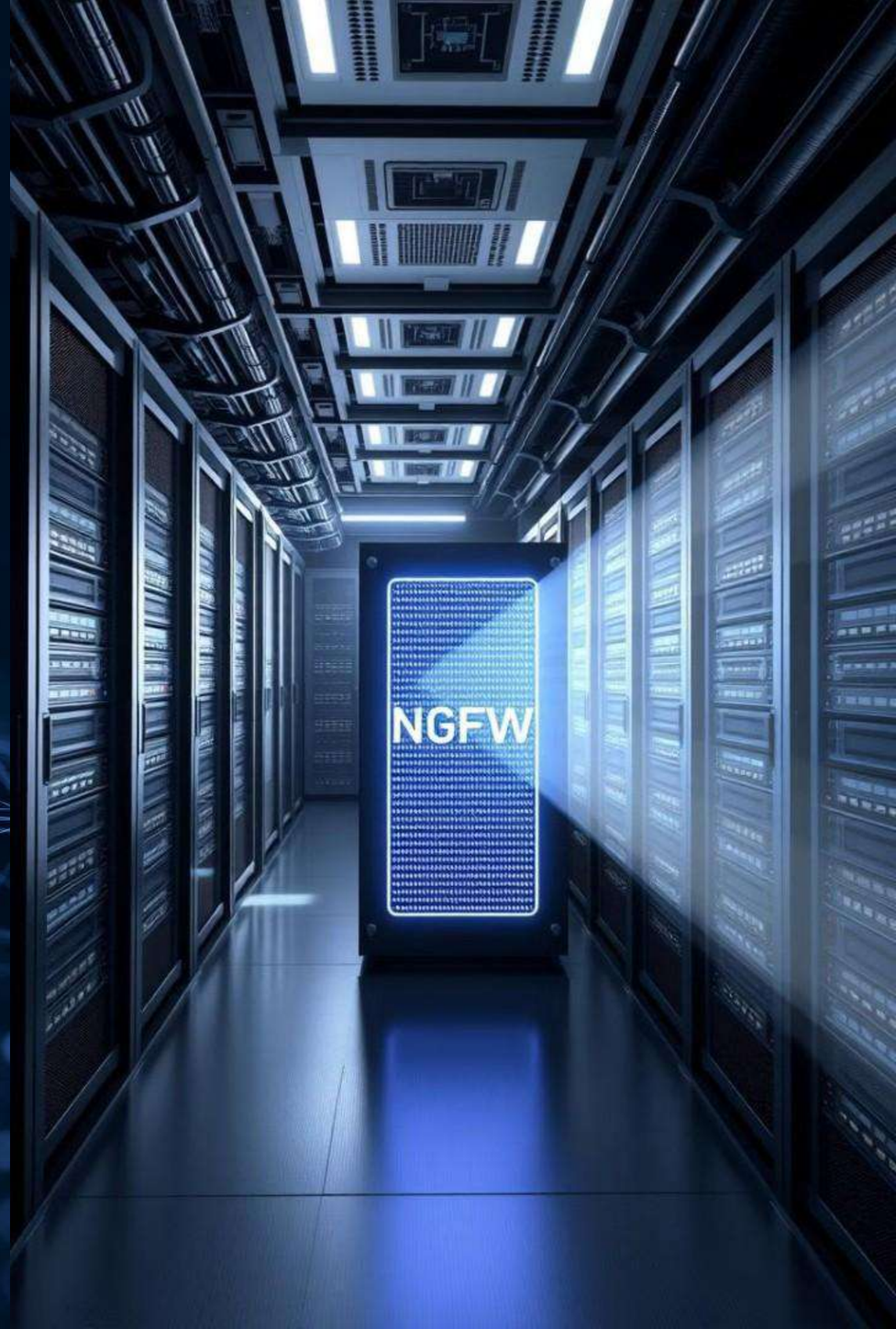
Поставьте барьер перед шифровальщиками и криптомайнерами. Предотвратите несанкционированное использование рабочих ресурсов: интернет-канала, ПО и сайтов, не помогающих выполнению служебных обязанностей.



Увеличьте эффективную скорость интернет-канала



До 40% трафика является «мусорным»: торренты, телеметрия Windows и spyware, баннеры, вирусы. Повысьте эффективное использование интернет-канала без затрат на его расширение.





Повысьте доступность ваших сервисов извне безопасно

Организуйте работу сотрудников в офисе из дома или в распределенной команде. Ваши коллеги смогут безопасно работать по VPN даже находясь в командировке: все важные задачи будут выполнены вовремя, а конфиденциальные данные останутся под контролем. Публикуйте веб-ресурсы и почтовый сервер, используя современные технологии защиты.

Модули QAZGATE

Контентная фильтрация

Контроль доступа в интернет с блокировкой 100 млн адресов в 146 категориях: "фишинг/мошенничество", "Центры распространения вредоносного ПО", "Ботнеты", "Тайный сбор информации", "Спам", "Реклама (баннеры)" и др.

Антивирусная проверка трафика

Потоковая проверка скачиваемых файлов и скриптов антивирусами Касперского и ClamAV. Блокировка вирусов до их попадания в локальную сеть.

Блокировка анонимайзеров

Блокировка попыток обхода системы контентной фильтрации с помощью прокси-серверов и плагинов для браузеров.

Контроль приложений (DPI)

Позволяет запретить определенным пользователям и группам трафик Skype, WhatsApp, YouTube, TikTok и др.

Предотвращение вторжений (IPS)

Блокирование атак, DoS, Spyware, телеметрии Windows, командных центров ботнетов, криптомайнеров, предупреждение вирусной активности внутри сети. Блокировка неблагонадежных регионов по GeoIP и IP-reputation.

Публикация ресурсов (WAF)

Защита внутренних веб-ресурсов с помощью Web Application Firewall при публикации их в интернете. Фильтрация и защита почтового трафика для опубликованных почтовых серверов.

Кому подойдет наше решение?

С числом интернет-пользователей от 50 до 10 000, использующих любые мобильные и десктопные ОС, включая отечественные.



Государственным и муниципальным учреждениям



Учебным заведениям: от ВУЗов до школ



Организациям с распределенной филиальной инфраструктурой



Коммерческим организациям



Промышленным предприятиям



Медицинским учреждениям

QazGate

Соответствует требованиям безопасности, установленным в СТ РК ISO/IEC 15408-3-2017 “Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты”. п.10, пп.11.1.4, 11.2.7, 11.3.4, 11.6.6, 12.1.4, 12.2.4, 13.1.7, 13.2.7, 13.3.4, 13.4.4, 13.6.4, 13.7.4, 14.1.5, 14.2.5,14.3.4, 14.4.5, 15.2.5. Оценочный уровень доверия 4.

Защита Вашей сети:

- Межсетевой экран
- VPN-сервер
- Контроль приложений
- Контентная фильтрация
- Предотвращение вторжений
- Центральная консоль

