Модель

# AZS8004-20

## Межсетевой экран нового поколения (NGFW)

Сравните интерфейсы устройств AZTCOFW. Выберите платформу с помощью рекомендаций команды по ресурсам и развёртыванию.

**8**
Ядра процессора

**32 GB**
ОЗУ

**До 1 TB SSD**
SSD-накопитель

## Оборудование для вашей сети.

| | |
|---|---|
| **Модель** | AZS8004-20 |
| **Ядра процессора** | 8 |
| **ОЗУ** | 32 GB |
| **SSD-накопитель** | До 1 TB SSD |
| **Сетевые интерфейсы** | 6 × 1 GbE RJ45; 2 × 1 GbE для управления; 4 × 10G SFP+ |

# Технические особенности сетевой границы.

Фильтрация, адресация, маршрутизация, VPN и отказоустойчивость для выбранной версии и схемы.

01

## Межсетевой экран с отслеживанием состояния

Фильтрация соединений IPv4 и IPv6 с учётом состояния. Настраивайте правила интерфейса и общие правила, разрешение/блокировку/отклонение, сети, порты и протоколы, журналирование и диагностику таблицы состояний.

02

## Организация политик

Повторно используйте псевдонимы узлов, сетей и портов, а также таблицы URL. Упорядочивайте правила, задавайте расписания и поддерживаемые лимиты подключений и состояний для каждого правила.

03

## NAT и публикация сервисов

Сопоставляйте внешний адрес внутреннему узлу через 1:1 NAT или публикуйте сервис переадресацией порта. Используйте автоматический, гибридный или ручной исходящий NAT, виртуальные IP и split DNS; доступ ограничивают правила.

04

## Сеть IPv6

Настраивайте двухстековые интерфейсы, статическую IPv6-адресацию или DHCPv6 на WAN, делегирование и отслеживание префиксов LAN, объявления маршрутизатора, SLAAC и DHCPv6. Правила IPv6 задаются отдельно от IPv4.

05

## Сегментация и маршрутизация

Создавайте интерфейсы VLAN 802.1Q, разделяйте LAN и DMZ, задавайте статические маршруты и маршрутизацию по шлюзам. Явно определяйте доступ между сегментами и совместно проверяйте виртуальные и физические коммутаторы.

06

## Несколько WAN

Контролируйте шлюзы, настраивайте многоуровневое переключение и балансировку новых соединений между шлюзами одного уровня. Выбор выполняется для соединения; существующей сессии может потребоваться повторное подключение.

# Технические особенности сетевой границы.

Фильтрация, адресация, маршрутизация, VPN и отказоустойчивость для выбранной версии и схемы.

07

### VPN-подключения

Используйте IPsec и OpenVPN для связи площадок и удалённого доступа; WireGuard доступен через совместимый пакет. Поддержка сертификатов, локальных учётных записей, RADIUS и LDAP зависит от выбранной схемы VPN.

08

### AZTCO HA

Обеспечьте переключение между совместимыми межсетевыми экранами с общими виртуальными адресами и синхронизацией состояний соединений и конфигурации. Выделите сеть синхронизации и уточните совместимость сервисов у реселлера.

09

### Управление трафиком

Настраивайте очереди формирования трафика и ограничители скорости загрузки/выгрузки, включая распределение по узлам. Поддерживаемая схема зависит от профилей полосы, драйверов интерфейсов и путей пакетов.

10

### Сетевые сервисы

Используйте DHCPv4/v6, ретранслятор DHCP при поддержке, DNS-resolver/forwarder, переопределения DNS, динамический DNS и NTP. Проверку DNSSEC можно включить в resolver.

11

### Идентификация и гостевой доступ

Управляйте локальными пользователями и правами, поддерживаемой аутентификацией RADIUS/LDAP, зонами captive portal и встроенными ваучерами/сессиями. Настройте оформление гостевого портала AZTCO.

12

### Конфигурация и восстановление

Управляйте через веб-интерфейс, создавайте и восстанавливайте резервную конфигурацию, просматривайте историю версий. Доступны управление сервисами, расписания и диагностика; для восстановления настроек дополнений могут потребоваться совместимые пакеты.

> Подберите модули и сервисы для вашей сети вместе с реселлером. Доступность зависит от лицензии, конфигурации устройства и выбранной версии ПО.

# От наблюдения за приложениями к явным правилам.

Проверьте обнаружение, область действия и применение политик до включения контроля.

01

### Политики приложений и категорий

Выбирайте поддерживаемые приложения или категории для наблюдения и контроля доступа. Точность обнаружения зависит от шифрования, изменений приложений и видимого межсетевому экрану трафика.

02

### Действия контроля

Сначала наблюдайте, затем разрешайте, блокируйте либо отдельно ограничивайте загрузку и выгрузку поддерживаемых потоков. Связанные с правилом межсетевого экрана политики проверяются по порядку.

03

### Область действия для клиентов и сетей

Связывайте политику приложения с правилами IPv4 и ограничивайте её узлами, сетями, именами хостов или псевдонимами адресов. Перед блокировкой проверьте соответствующий путь трафика.

04

### Интеграция с правилами межсетевого экрана

Сохраняется приоритет встроенного порядка правил. Управляемые назначения приложений можно использовать с упорядоченными правилами и шлюзами; позднее обнаружение не перенаправляет уже начатый поток.

05

### Актуальные определения приложений

Управляемые определения имён хостов и доменов дополняют анализ протоколов для поддерживаемых приложений. Общие IP, изменения CDN, шифрование имён и туннели могут снизить точность классификации.

06

### Обновление детекторов

Обновляйте проверенные региональные данные вручную либо ежедневно/еженедельно по UTC. Состояние видно, предыдущий набор сохраняется. По умолчанию расписание выключено.

07

### Операционная видимость

Просматривайте обнаруженные потоки приложений, байты, пакеты и решения политик. Данные доступны в совместимых представлениях Traffic Center и Client Risk, но не являются полным архивом трафика.

08

### Ограничения развёртывания

Классификации нужен наблюдаемый трафик, она может начаться после первых пакетов. Перед блокировкой проверьте рабочие приложения, шифрование, VPN и формирование трафика. Политики приложений, связанные с правилами, поддерживают IPv4.

> Без проверки HTTPS WebGuard применяет политику назначения по запрошенному имени хоста. Для антивирусной проверки нужны проверяемый HTTPS-трафик и доверенный клиентский сертификат.

# Средства защиты с учётом рабочих процессов.

Узнайте назначение модулей, их место в сети и условия, которые следует учесть при развёртывании.

01

## AZTCO IPS-IDS

Сигнатурная проверка, политики по интерфейсам, выбранные категории правил, исключения, оповещения и просмотр заблокированных узлов. Доступ к сигнатурам, обновление и предотвращение зависят от лицензии и настройки.

02

## DNS Blocker

Используйте списки репутации DNS/IP, разрешённые исключения и выбор источников для ограничения нежелательных или рискованных назначений. Политика действует для запросов через настроенный resolver; альтернативный и шифрованный DNS требуют сетевых правил.

03

## WebGuard

Контролируйте доступ через явный HTTP/HTTPS-прокси с упорядоченными правилами доменов, областями клиентов и расписаниями. Кэшируйте подходящие HTTP-ответы и включайте проверку HTTPS с исключениями при доверенном сертификате на клиентах.

04

## Антивирус

Проверяйте подходящие HTTPS-загрузки через инспекцию WebGuard и блокируйте обнаруженное вредоносное ПО. Необходимы инспекция HTTPS и доверие клиента к сертификату проверки.

05

## Client Risk

Сопоставляйте поддерживаемые события IPS, DNS, межсетевого экрана и приложений. Анализируйте оценки риска 0–100, историю доказательств, заметки и ответственных. Настраивайте временное доверие, уведомление/блокировку или ограниченный карантин. Оценка указывает на подозрение, а не подтверждённый взлом.

06

## Traffic Center

Отслеживайте наблюдаемую загрузку/выгрузку клиентов и приложений, текущую активность, итоги интерфейсов и ежедневные отчёты. Экспортируйте CSV и включайте почту по желанию. Не складывайте вместе итоги клиента и интерфейса.

07

## Группы FreeRADIUS и Captive Portal

Объединяйте локальных пользователей и зарегистрированные устройства в группы; используйте псевдонимы групп IPv4 в правилах доступа. Создавайте брендированные гостевые страницы для зон, редактируйте, просматривайте и публикуйте их.

08

## Hotspot Guard

Отслеживайте выбранные клиентские интерфейсы на признаки совместного подключения, проверяйте основания и исключения, выбирайте уведомление или ограничение источника. Результаты требуют проверки и сами по себе не доказывают совместный доступ.

09

## Разгрузка SSL

Публикуйте сервисы через обратный прокси с завершением TLS, настройкой frontend/backend, проверками состояния, балансировкой серверов и статистикой через совместимую интеграцию HAProxy. Она не заменяет WAF.

# Подключите действующую систему мониторинга.

Используйте локальную диагностику вместе со своим сборщиком журналов, SIEM и системой управления сетью.

01

### Системные журналы и журналы межсетевого экрана

Просматривайте события экрана, системы, аутентификации, VPN, DNS/DHCP и шлюзов. Передавайте журналы на внешний syslog-сборщик для хранения вне устройства; встроенная отправка использует UDP.

02

### Структурированные события безопасности

Отправляйте события Client Risk по syslog через UDP, TCP или TLS. TCP/TLS используют octet-counted framing; TLS проверяет сертификат приёмника. Выбирайте события безопасности, политик и администрирования/состояния.

03

### Опрос SNMP

Передавайте поддерживаемые системные сведения и интерфейсы во внешнюю систему управления сетью через встроенный SNMP. Ограничьте доступ разрешёнными узлами мониторинга и проверьте MIB выбранного выпуска.

04

### Ловушки SNMP

Client Risk отправляет ловушки SNMPv2c с ID события, адресом клиента, действием и оценкой риска. Настройте приёмник, community и выделенную базу корпоративного OID. Ловушки не добавляют OID для опроса; модуль не поддерживает SNMPv3/informs.

05

### Трафик и шлюзы

Графики/счётчики интерфейсов, задержка и потери шлюзов, состояния экрана, маршруты и статус VPN помогают отличить сбой канала от проблемы политики или сервиса.

06

### Средства диагностики

Используйте захват пакетов, ping, traceroute, DNS-запросы, просмотр маршрутов/состояний и совместимый Speedtest для поиска неисправностей. Учитывайте нагрузку рабочей сети.

07

### AI Diagnostics

Запускайте локальные пошаговые проверки, сопоставляющие состояние, конфигурацию и клиентские данные. Результат обьясняет наблюдаемые признаки; оператор проверяет его до изменения политики.

08

### Отчёты и уведомления

Просматривайте историю и доказательства Client Risk, отчёты CSV/печати, ежедневное использование Traffic Center и экспорт CSV. Почта доступна при настроенном SMTP; состав отчёта зависит от наблюдений и хранения.

09

### Интеграция сборщиков

Передавайте поддерживаемые журналы и события в SIEM или систему мониторинга. На приёмнике настройте разбор, время, хранение и обработку дублей. UDP и ловушки не подтверждают доставку; очереди ограничены.

# Проверяйте лицензию и планируйте поддержку.

Проверяйте срок действия и продление, а также резервные копии конфигурации при включённой функции.

01

### Портал клиента

Проверяйте лицензии экранов, даты окончания и продления в одном месте. Если включено резервное копирование, просматривайте сохранённые копии и скачивайте доступные согласно правам аккаунта.

02

### Резервные копии конфигурации

Храните копии конфигурации вне устройства для восстановления. При включении для подключённого экрана плановые и версионные копии помогают восстановить или заменить его на совместимой системе.

03

### Техническая поддержка

Получайте помощь с конфигурацией, соединением, VPN, настройкой политик и диагностикой. Удалённая помощь предоставляется по применимому плану и с вашего согласия.

04

### Ответ и эскалация

Согласуйте часы поддержки, уровни серьёзности, целевые сроки первого ответа и контакты эскалации. Объём услуг задаёт договор; время ответа и срок решения различаются.

05

### Онлайн-обновления

Устанавливайте доступные исправления и улучшения, проверяйте разрешённые лицензией версии, состояние и историю обновлений. Планируйте установку в окна обслуживания.

06

### Офлайн-обновления

Обновляйте изолированные или ограниченные по Интернету системы автономными пакетами без прямой загрузки с межсетевого экрана. Уточните наличие пакетов и порядок переноса для выбранного выпуска.

07

### Гибкость обслуживания

Выбирайте подключённое или автономное обслуживание с учётом сетевых правил. Планируйте обновления и перезапуски с командой или поддержкой AZTCO и уточняйте наличие пакетов для выпуска.

08

### Ремонт и временная замена оборудования

При отказе оборудования, включённого в обслуживание, обратитесь в поддержку для диагностики, ремонта или замены согласно договору. При наличии может быть предоставлено временное устройство, чтобы сохранить основную ёмкость на время ремонта. Доступность, доставка и условия зависят от региона и плана; уточните покрытие до покупки.

# Запросить предложение

Обсудите сеть с AZTCOFW или реселлером. Мы поможем выбрать ПО, способ развёртывания и подходящую поддержку. · **AZS8004-20**

## Расскажите о ваших требованиях

### Развёртывание

AZS8004-20 · 8 Ядра процессора · 32 GB ОЗУ · До 1 TB SSD

### Сеть и защита

6 × 1 GbE RJ45; 2 × 1 GbE для управления; 4 × 10G SFP+. Число пользователей, скорость Интернета, интерфейсы, VPN-подключения и необходимые модули защиты.

### Поддержка

Требования к поддержке, AZTCO HA или резервная VM, а также временная замена оборудования при наличии.

### Запросить расчёт ресурсов и стоимости VM

Цена VM-лицензии рассчитывается по требуемым ресурсам CPU (выделенным vCPU/ядрам) и количеству сетевых интерфейсов. В предложении указываются лимит ресурсов, срок и опции.

## Контакты

Обсудить со специалистом aztcofirewall.com/ru/contact?interest=AZS8004-20

Скачать описание продукта (PDF)