ATP100-RU0112F

Серия ATP - Бескомпромиссная и унифицированная защита сети.

Межсетевой экран Zyxel ATP100, 1xWAN GE, 1xOPT GE (LAN/WAN), 3xLAN/DMZ GE, 1xUSB3.0, Контроллер точек доступа WiFi (8 устройств в базе, 24 – с лицензией), NebulaFlex Pro.

Идет в комплекте, с подпиской Gold на 1 год (AS, AV, CF, IDP/DPI, Sandboxing, SecuReporter, Secure Wi-Fi, 24 AP).

Серия Zyxel ZyWALL ATP — это межсетевые экраны, предназначенные для малого и среднего бизнеса и оснащенные интеллектуальными функциями, которые повышают уровень защиты сети, особенно при борьбе с неизвестными угрозами. Эта серия поддерживает не только все сервисы безопасности Zyxel, такие как контентная фильтрация, патруль приложений, антиспам, репутационный фильтр и т. д., но также песочницу и сервис аналитики SecuReporter, обеспечивающие высокую производительность и комплексную защиту как саморазвивающееся решение.

Эффективная совместная работа с серией ATP

Расширение портфолио устройств Nebula с помощью межсетевых экранов ATP обеспечивает совместную защиту сети и проверку файлов в песочнице. Получайте подробные отчеты для активного мониторинга и высокой видимости сетевой активности с нашей постоянно развивающейся защитой.

Комплексное обнаружение и предотвращение угроз

ATP оснащен несколькими инструментами защиты, такими как песочница, чтобы остановить неизвестное вредоносное ПО и угрозы нулевого дня, и CDR, который может блокировать или помещать в карантин скомпрометированных клиентов на границе сети, сдерживая угрозу и предотвращая дальнейший ущерб.

Единая безопасность во всех сетях

Мы предлагаем широкий спектр продуктов, которые обеспечивают различные варианты удаленного доступа, включая межсетевые экраны для головного офиса и филиалов, точки удаленного доступа с Secure Wi-Fi и

VPN клиенты для удаленных сотрудников, расширяя защиту конечных устройств.

Оптимизация использования ресурсов

ATP может помочь бизнесу управлять тем, какие приложения используют сотрудники, и быстро просматривать все приложения за определенный период. Более 3700 приложений классифицируются по различным меткам. Просто наведите курсор, чтобы заблокировать или разблокировать любое из них.

Централизованное управление Nebula

- **Гибкое и масштабируемое решение**
  Реселлеры, поставщики услуг и сетевые администраторы оценят простоту, масштабируемость, гибкость и снижение затрат благодаря платформе централизованного управления Zyxel Nebula.

- **Подключение без лишних сложностей**
  Nebula предоставляет мощное, легкое и удобное решение, которое работает с различным оборудованием от Zyxel, устраняя сложности и риски безопасности, часто связанные с использованием оборудования от разных вендоров.

- **Запуск сети за считанные минуты**
  Подключайте, защищайте и управляйте безопасностью, коммутацией, Wi-Fi, а также LTE/5G через нашу централизованную платформу Nebula.

- **Обширное портфолио устройств**
  Zyxel не имеет себе равных в своем подходе к внедрению новых и существующих продуктов в Nebula, на данный момент свыше 80 моделей устройств поддерживают её. От развертывания домашнего офиса до распределенной сетевой архитектуры — портфолио продуктов Zyxel с поддержкой Nebula может удовлетворить любой бюджет, функциональность и масштабируемость как сейчас, так и в будущем.

Функциональность

Машинное обучение

Облако Zyxel идентифицирует неизвестные файлы на основе запросов от всех межсетевых экранах ATP, которые используются по всему миру, и сохраняет всю информацию о каждой новой обнаруженной угрозе. Zyxel Cloud функционирует как непрерывно растущая и постоянно саморазвивающаяся база данных о защите от угроз, которая непрерывно учится, растет и эволюционирует.

- **Песочница**
  Песочница (Sanboxing) изолирует подозрительные файлы для их проверки на наличие новых типов вредоносного кода, которые нельзя выявить с помощью традиционных механизмов статичной защиты. Песочница гарантирует защиту от атак "нулевого дня".

- **Машинное обучение новым угрозам**
  Функционал машинного обучения ежедневно синхронизируется со всеми межсетевыми экранами ATP, поэтому каждый ATP получает преимущества машинного обучения в облаке. Облако и межсетевые экраны ATP образуют экосистему безопасности, в которой они вместе обучаются и усиливают свою защиту, поэтому они всегда защищены от новых еще неизвестных атак. Интеллектаульное облако постоянно расширяется и эволюционирует за счет слияния многих баз данных, её растущий багаж знаний об угрозах позволяет ATP в реальном времени обнаруживать вредоносный код.

Многоуровневая защита
Межсетевой экран ATP использует многоуровневую защиту от внешних и внутренних угроз. Песочница, антивирус, репутационный фильтр и предотвращение вторжений блокируют атаки извне, а патруль приложений и контентная фильтрация позволяют ограничить права пользователей на запуск посторонних приложений или доступ к сайтам. Весь этот функционал защитит вашу сеть и закроет все дыры в её системе безопасности.

- Гео-идентификация
- Веб-безопасность
- Безопасность приложений
- Облачная песочница
- Антивирус
- Предотвращение вторжений (IDP)
- Репутационный фильтр

Репутационный фильтр IP/DNS/URL

Репутационный фильтр, включающий проверку по IP, DNS и URL, сопоставляет IP-адреса/домены/URL-адреса с постоянно обновляемой базой данных и определяет, является ли адрес заслуживающим доверия или нет. Это повышает эффективность блокировки, ограничивает доступ к вредоносным доменам/URL-адресам, а также блокирует доступ из скомпрометированных источников, обеспечивая тем самым детальную защиту от постоянно развивающихся киберугроз.

Комплексная веб-фильтрация

ATP обеспечивает расширенные функциональные возможности веб-фильтрации и безопасность благодаря мощному сочетанию фильтрации на основе категорий и репутации. Динамический анализ содержимого сайтов определяет, принадлежит ли он к нежелательной категории, например азартные игры, порнография, игры и многое другое. Недавно добавленный контент-фильтр по DNS предлагает лучший подход к проверке доступа в Интернет, особенно когда веб-сайт использует ESNI (зашифрованное указание имени сервера), где традиционная фильтрация URL-адресов не применима к домену назначения.

Глубокий анализ всех ваших устройств

Анализ устройств (Device Insight) дает вам больше информации о ваших сетях, включая проводные, беспроводные, BYOD и IoT-устройства. Вы можете создать политику доступа с контекстом, например с версией ОС или категорией устройства, чтобы обеспечить сегментацию сети. Это уменьшает вероятность атаки и предотвращает распространение угроз. Это также помогает сократить время, затрачиваемое на исследование угроз. Продолжая стремиться к повышению прозрачности работы клиентов, Zyxel SecuReporter предоставляет вашей организации комплексную панель управления конечных устройств.

Сервис анализа и отчетов

Панель управления ATP предоставляет удобную инфографическую сводку трафика и статистику угроз. Пользователи также могут использовать SecuReporter для дальнейшего всестороннего анализа угроз.

Панель управления

Панель управления ATP предоставляет статистику угроз за семь дней и сводку трафика с момента перезагрузки, обеспечивая быстрый обзор сетевой безопасности.

SecuReporter

SecuReporter предлагает комплексный анализ логов с корреляцией данных и предоставляет настраиваемые отчеты, необходимые для MSP и поставщиков дополнительных услуг.