ZYXEL

ZyWALL ATP100/200/500/800

Межсетевой экран ATP

Межсетевой экран следующего поколения для SMB

Zyxel ZyWALL ATP100/200/500/800 – это серия межсетевых экранов с расширенной защитой от угроз, специально разработанных для малого и среднего бизнеса, в которых используется облачный интеллект для надежной защиты сетей, в том числе от неизвестных угроз. Серия ZyWALL ATP поддерживает все сервисы безопасности Zyxel: контентную фильтрацию, патруль приложений, антиспам, репутационный фильтр, а также «песочницу», аналитический сервис SecuReporter и веб-интерфейс с инфографикой, представляя собой саморазвивающееся решение, обеспечивающее высокую производительность и эффективность защиты сети.

- Облачный интеллект с машинным обучением и глобальной базой данных об угрозах
- Песочница для защиты от неизвестных угроз
- Отчеты и аналитика в облаке и на устройстве
- Надежная многоэшелонная защита

Техническая спецификация ZyWALLATP100/200/500/800

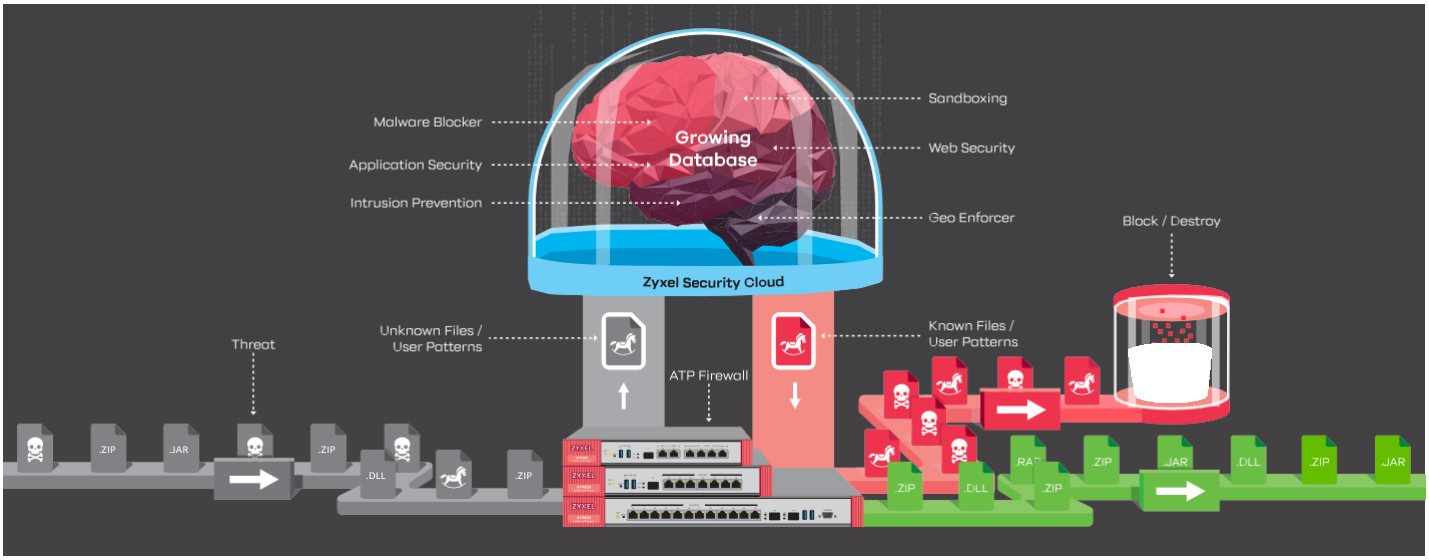
Преимущества

Саморазвивающийся облачный интеллект

Облачный интеллект получает все неизвестные файлы или паттерны пользователей из запросов от всех межсетевых экранов Zyxel ATP, затем при помощи машинного обучения идентифицирует потенциальные угрозы и записывает в архив результаты этого анализа. После этого все межсетевые экраны ATP получают сигнатуры самых опасных угроз, поэтому все устройства ATP надежно защищают от новых ранее неизвестных угроз. Благодаря синхронизации в реальном времени база сигнатур облачного интеллекта постоянно растет, образуя саморазвивающуюся экосистему безопасности, которая адаптируется к атакам извне и постоянно синхронизируется со всеми установленными межсетевыми экранами ATP.

В песочнице эмулируются неизвестные угрозы

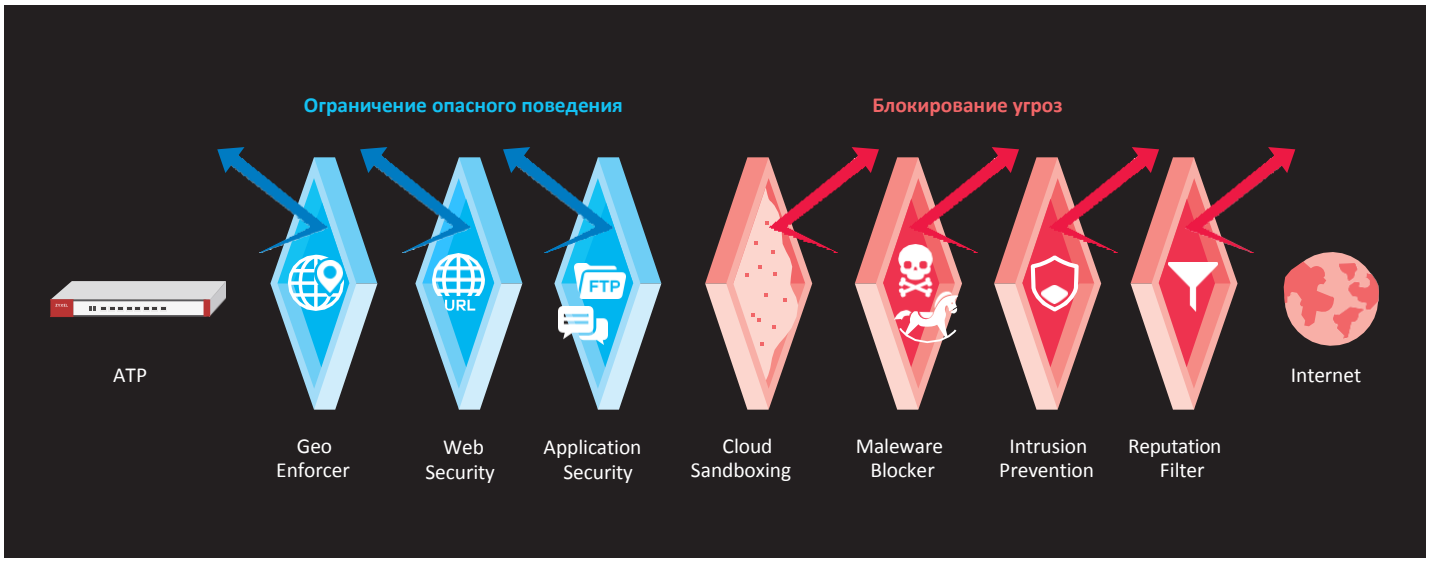
«Песочница» (Sanbdoxing) - это изолированная среда в облаке, в которой содержатся неизвестные файлы. Эти файлы не удается идентифицировать с помощью сервисов безопасности устройства, поэтому в песочнице эмулируется их поведение, чтобы определить, являются ли они опасными. Главное назначение песочницы – это инспекция поведения пакетов в изолированной среде, при котором в сеть не может попасть потенциальная угроза. Она позволяет идентифицировать новые типы угроз, которые не способны обнаружить традиционные статичные механизмы защиты. Использование облачной песочницы в устройствах серии Zyxel ATP обеспечивает превентивную защиту от любых угроз нулевого дня (zero-day).



Надежная многоэшелонная защита

Традиционные специализированные решения рассчитаны на отражение атак определенно типа, но вредоносный код постоянно совершенствуется и может проникнуть в сеть на любом этапе атаки, поэтому традиционные средства защиту становятся неэффективными. В серии ZyWALL ATP используется многоэшелонная защита, обеспечивающая отражение атак по разным направлениям как извне, так и внутри сети.

В этих межсетевых экранах применяются мощные функции безопасности, в том числе фильтр ботнет-сетей, песочница, патруль приложений, фильтры контента и репутации, антивирус и IDP. Сразу же после запуска межсетевой экран ATP включает защиту вашей сети и ликвидирует все слабые места в её системе безопасности.



Репутационный фильтр – превентивная защита

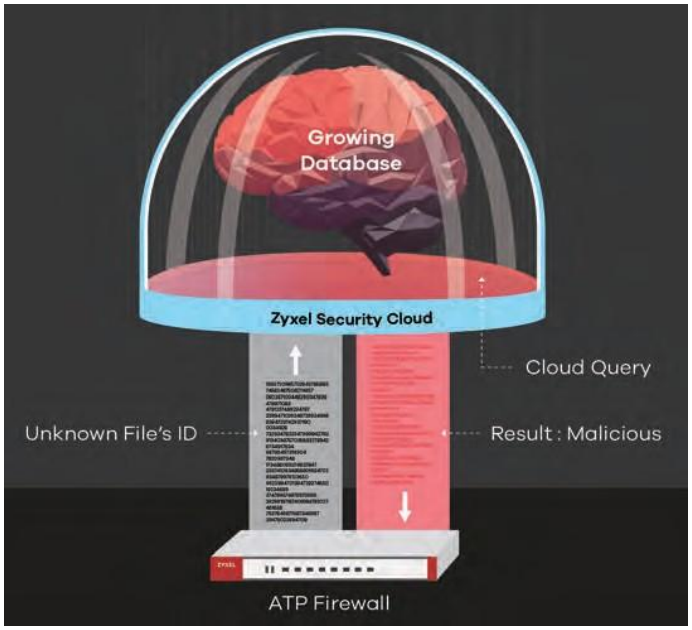
Репутационный фильтр проверяет IP-адреса по обновляемой в реальном времени облачной базе данных, в которую заносится информация о кибератаках, и на основе этой проверки определяет, можно ли доверять IP-адресу. Применение этой функции улучшает эффективность блокировки, сокращает загруженность оборудования, предоставляя администратору дополнительные сетевые ресурсы, чтобы легко и оперативно решать любые проблемы. Репутационный фильтр также улучшает выявление угроз в SecuReporter (входит в комплект лицензий) и помогает установить источники угроз.

Cloud Query выводит защиту ATP на новый уровень

Когда появляется новый файл, то за несколько секунд облачный запрос (Cloud Query) проверяет его ID по базе данных в Zyxel Security Cloud и сразу определяет, является ли файл опасным. Во время этой операции используется минимум пропускной способности сети, но обеспечивается ее надежная защита с применением нескольких баз сигнатур, содержащих огромный объем данных о угрозах и постоянно расширяющихся за счет информации от облачного машинного обучения. Cloud Query также ускоряет сбор информации о новых угрозах с помощью Zyxel Security Cloud и тем самым усиливает защиту каждого межсетевого экрана ATP.

Аналитика и отчеты о неизвестных угрозах

Веб-интерфейс межсетевых экранов ATP отображает в удобном для восприятия графическом формате сводку о трафике и статистику угроз. В облачный аналитический сервис SecuReporter включены различные инструменты аналитики и генерации отчетов, включая идентификацию и анализ сетевых угроз, отчеты от сервисов безопасности об использовании приложений, web-сайтов и трафика. Можно проанализировать детальную информацию о результатах работы песочницы и при необходимости отправить предупреждение администратору по e-mail. Фильтр ботнет-сетей выводит список самых опасных web-сайтов, зараженных ботами, и тип ботов. Аналитика репутационного фильтра отображает информацию об IP-адресах, которые были использованы для атак. Серия ATP с SecuReporter обеспечивает полную защиту и мощные средства анализа угроз.



Сервисы и лицензии

Межсетевые экраны серии ZyWALL ATP поддерживают все основные функции защиты, поэтому подойдут для любых задач бизнеса, а также обеспечивают получение максимума производительности и безопасности с помощью одного универсального устройства. Модульная архитектура этих сетевых экранов позволяет IT-специалисту настроить конфигурацию в соответствии со своими потребностями.

Sandboxing

Web Security

Application Security

Malware Blocker

Intrusion Prevention

Reputation Filter

Geo Enforcer

Managed AP service

SecuReporter

Пакеты лицензий

Лицензируемый сервис	Функция	ZyWALL ATP100/200/500/800[*1]
		Gold Security Pack (1 год/2 года)
Sandboxing	Песочница	Да
Web Security	Контентная фильтрация	Да
	Фильтр ботнет-сетей	Да
Application Security	Патруль приложений	Да
	Антиспам	Да
Malware Blocker	Антивирус	Да
	Cloud Query (облачный запрос)	Да
	Интеллектуальное машинное обучение	Да
Intrusion Prevention	Обнаружение и предотвращение вторжений	Да
Reputation Filter	Репутационный фильтр	Да
Geo Enforcer	Геополитики	Да
Managed AP Service[*2]	Контроллер точек доступа	Максимальное число точек доступа
SecuReporter	SecuReporter Premium	Да

*1: Все модели ATP по умолчанию поставляются с лицензией Gold Security Pack на 1 год. Этот пакет лицензий нельзя передавать (non-transferable).
*2: Gold Pack обеспечивает управление 10 и более точками доступа в течение одного года (10 точек доступа для ATP100, 18 точек доступа для ATP200, 34 точки доступа для ATP500, 130 точек доступа для ATP800), по истечении лицензии можно управлять только 2 точками доступа.

Спецификации

Модель	ZyWALL ATP100	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
Фотография продукта				
Спецификация оборудования				
Порты 10/100/1000 Mbps RJ-45/SFP	4 x LAN/DMZ, 1 x WAN, 1 x SFP	4 x LAN/DMZ, 2 x WAN, 1 x SFP	7 (конфигурируемые), 1 x SFP	12 (конфигурируемые), 2 x SFP (конфигурируемые)
Порты USB 3.0	1	2	2	2
Консольный порт	Да (RJ-45)	Да (DB9)	Да (DB9)	Да (DB9)
Монтаж в стойке	-	Да	Да	Да
Без вентилятора	Да	Да	-	-
Емкость и производительность *1				
Пропуск. способность межсет. экрана SPI (Мбит/сек) *2	1 000	2 000	2 600	8 000
Пропускная способность VPN (Мбит/сек) *3	300	500	900	1 500
Пропускная способность IDP (Мбит/сек) *4	600	1 200	1 700	2 700
Пропускная способность AV (Мбит/сек) *4	250	450	700	1 200
Пропускная способность UTM (AV и IDP) *4	250	450	700	1 200
Максимальное число одновременных сессий TCP *5	300 000	600 000	1 000 000	2 000 000
Максимальное число туннелей IPSec VPN *5	40	40	200	1 000
Максимальное число туннелей SSL VPN	10	10	50	100
Кол-во интерфейсов VLAN	8	16	64	128
Производительность в Speedtest на канале 1 Гбит/с				
Пропуск. способность межсет. экрана SPI (Мбит/сек) *6	850	900	900	930
Контроллер точек доступа				
Число управляемых точек доступа (лицензия на 1 год) *7	10	18	34	130
Сервисы безопасности *8				
Sandboxing	Да	Да	Да	Да
Web Security	Да	Да	Да	Да
Application Security	Да	Да	Да	Да
Malware Blocker	Да	Да	Да	Да
Intrusion Prevention (IDP)	Да	Да	Да	Да
Reputation Filter	Да	Да	Да	Да
Geo Enforcer	Да	Да	Да	Да
SecuReporter	Да	Да	Да	Да
Основные функции				
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
SSL (HTTPS) инспекция	Да	Да	Да	Да
2-факторная аутентификация	Да	Да	Да	Да
Microsoft Azure	Да	Да	Да	Да
Amazon VPC	Да	Да	Да	Да
Device HA Pro	-	-	Да	Да

Модель		ZyWALL ATP100	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
Требования к питанию					
Источник питания		12 В постоянного тока, максимум 2 А	12 В постоянного тока, максимум 2.5 А	12 В постоянного тока, максимум 4.17 А	100-240 В переменного тока, 50/60 Гц, максимум 2.5 А
Максимальное энергопотребление (Ватт)		12.5	13.3	24.1	46
Тепловыделение (BTU/час)		42.65	45.38	82.23	120.1
Физические характеристики					
Без упаковки	**Размеры (ШхГхВ) (мм):**	216 x 143 x 33	272 x 187 x 36	300 x 188 x 44	430 x 250 x 44
	Вес (кг)	0.85	1.4	1.65	3.3
В упаковке	**Размеры (ШхГхВ) (мм):**	284 x 190 x 100	427 x 247 x 73	351 x 152 x 245	519 x 392 x 163
	Вес (кг)	1.4	2.23 (без скоб) 2.42 (со скобами)	2.83	4.8
Аксессуары в комплекте поставки		• Адаптер питания • Кабель RJ-45 • Кабель RS-232	• Адаптер питания • Набор для монтажа в стойке	• Адаптер питания • Силовой кабель • Набор для монтажа в стойке	• Силовой кабель • Набор для монтажа в стойке
Требования к окружающей среде					
Эксплуатация	**Температура**	0°C - +40°C	0°C - +40°C	0°C - +40°C	0°C - +40°C
	Относительная влажность	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)
Хранение	**Температура**	-30°C - +70°C	-30°C - +70°C	-30°C - +70°C	-30°C - +70°C
	Относительная влажность	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)	10% -90% (без выпадения конденсата)
MTBF (часов)		989 810.8	529 688.2	529 688.2	947 736
Акустический шум		-	-	24.5 дБА при работе с t< 25°C, 41.5 дБА при максимальной скорости вращения вентилятора.	25.3 дБА при работе с t< 25°C, 41.5 дБА при максимальной скорости вращения вентилятора.
Сертификаты					
EMC		FCC Part 15 (Class B), CE (Class B), RCM (Class B), BSMI	FCC Part 15 (Class B), CE (Class B), RCM (Class B), BSMI	FCC Part 15 (Class A), CE (Class A), RCM (Class A), BSMI	FCC Part 15 (Class A), CE (Class A), RCM (Class A), BSMI
Безопасность		LVD, BSMI	LVD, BSMI	LVD, BSMI	LVD, BSMI

*: Эта таблица для микропрограммы ZLD4.35 и более поздней версии.

*1: На практике производительность может быть меньше из-за условий работы сети и активных приложений.

*2: Максимальная пропускная способность в соответствии с RFC 2544 (UDP-пакеты по 1518 байтов).

*3: Пропускная способность VPN в соответствии с RFC 2544 (UDP-пакеты по 1424 байта).

*4: Пропускная способность AVP и IDP измерялась с помощью стандартной утилиты тестирования производительности HTTP (пакеты HTTP по 1460 байтов). Тестирование производилось с несколькими потоками.

*5: Максимальное число сессий измерялось с помощью стандартной утилиты тестирования IXIA 1xLoad.

*6: Тесты Speedtest проводили с использованием канала 1 Гбит/с в реальной сети, и на их результаты может повлияет качество канала сервис-провайдера.

*7. По истечении срока действия лицензии Gold Pack поддерживается только 2 точки доступа.

*8: для использования этой функции и расширения ее емкости нужна лицензия Zyxel.

Список совместимых точек доступа

Продукт	Точки доступа Unified		Точки доступа Unified Pro	
Модели	• NWA5121-N • NWA5121-NI • NWA5123-AC • NWA5123-AC HD • NWA5123-NI	• NWA5301-NJ • WAC5302D-S • Совместимые точки доступа*	• WAC6103D-I • WAC6303D-S • WAC6502D-E • WAC6502D-S • WAC6503D-S	• WAC6552D-S • WAC6553D-E • Совместимые точки доступа*
Функции				
Централизованное управление	Да		Да	
Автонастройка	Да		Да	
Передача данных	Локальная		Локальная/туннельная	
ZyMesh	Да		Да	

*: Начиная с версии контроллера APC3.0, межсетевые экраны могут распознавать точки доступа, использующие микропрограмму новее APC3.0, как совместимые точки доступа. Реселлеры могут продвигать новые точки доступа Zyxel с поддержкой базовых функций без обновления микропрограммы контроллера.

Функции программного обеспечения

Сервисы безопасности

Межсетевой экран

- Сертифицированный ICSA межсетевой экран корпоративного класса
- Режимы маршрутизатора и моста
- Инспекция пакетов с хранением состояния
- Применение политик с учетом конкретного пользователя
- SIP/H.323 NAT traversal
- Поддержка ALG для настраиваемых портов
- Обнаружение и защита от аномалий протоколов
- Обнаружение и защита от аномалий трафика
- Обнаружение и защита от флуда
- Защита от DoS/DDoS атак

Унифицированные политики безопасности

- Унифицированный интерфейс управления политиками
- Поддержка контентной фильтрации, патруля приложений, межсетевого экрана (ACL/SSL)
- Критерии политики: зоны, IP-адреса назначения/источника, пользователи, время

Обнаружение и предотвращение вторжений (IDP)

- Режим маршрутизатора и моста
- Сканирование по сигнатурам и поведению
- Поддержка пользовательских сигнатур
- Автоматическое обновление сигнатур

Патруль приложений

- Гранулярный контроль самых важных приложений
- Идентификация и контроль поведения приложений
- Поддержка 30+ категорий приложений
- Поддержка аутентификации пользователей
- Статистика и отчеты в реальном времени

Sandboxing (песочница)

- Инспекция в облаке с применением различных механизмов
- Поддержка HTTP/SMTP/POP3/FTP
- Проверка различных типов файлов
- Синхронизация базы данных угроз в реальном времени

Антивирус

- Потоковый механизм сканирования
- Отсутствие ограничений на размер файла
- Поддержка протоколов HTTP, FTP, SMTP, POP3
- Автоматическое обновление сигнатур

Cloud Query (облачный запрос)

- Облачный механизм сканирования
- Использование постоянно растущей базы данных с 30+ млрд сигнатур
- Поддержка протоколов на базе FTP/HTTP/HTTPS
- Поддержка различных типов файлов

Антиспам

- Прозрачный перехват почты с использованием протоколов SMTP и POP3
- Репутационный фильтр IP-адресов отправителей
- Обнаружение спама, фишинга, вирусов
- Черный и белый список адресов
- Поддержка проверки DNSBL

Репутационный фильтр

- Фильтр репутации на базе IP-адресов
- Поддержка 10 категорий киберугроз
- Фильтр входящего/исходящего трафика
- Черный и белый список адресов

Фильтр ботнет-сетей

- Блокирование web-сайтов ботнета
- Блокирование опасных URL-адресов

Контентная фильтрация

- Фильтр доменов HTTPs
- Поддержка SafeSearch (безопасный поиск)
- Применение белого списка web-сайтов
- Черный и белый список URL, блокировка по ключевым словам
- Настраиваемые предупреждения и URL-перенаправление

Геополитики

- Блокирование IP-адресов по геопризнаку
- География адресов для статистики трафика и логов
- Поддержка адресов IPv6

IP-исключения

- Гранулярный контроль IP-адресов отправителей и получателей
- Поддержка списков исключений для IDP и антивируса

VPN

IPSec VPN

- Управление ключами: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Шифрование: DES, 3DES, AES (256-bit)
- Аутентификация: MD5, SHA1, SHA2 (51-2bit)
- Поддержка PFS (DH группы) 1, 2, 5, 14, 15-18
- Поддержка сертификатов PSK и PKI (X.509)
- IPSec NAT traversal (NAT-T)
- Dead Peer Detection (DPD) и обнаружение повторных пакетов
- VPN концентратор
- Маршрутизируемые туннельные интерфейсы (VTI)
- Балансировка и резервирование VPN
- GRE over IPSec
- NAT over IPSec
- L2TP over IPSec
- Настройка клиентов Zyxel VPN
- Поддержка клиентов iOS для L2TP/IKE/IKEv2 VPN

SSL VPN

- Поддержка Windows и Mac OS X
- Поддержка режима полного туннелирования
- Поддержка 2-факторной аутентификации

Сеть

Контроллер WLAN

- Поддержка контроллера (APC) v3.40
- Поддержка протоколов 802.11k/v/r
- Изоляция на уровне L2
- Поддержка автоматического обновления микропрограмм точек доступа
- Включение Wi-Fi по расписанию
- Динамический выбор каналов (DCS)
- Приоритезация 5 GHz диапазона
- Автопокрытие зон отключенных точек доступа
- Настраиваемый web-портал авторизации
- Поддержка Wi-Fi Multimedia (WMM) QoS
- Поддержка протокола обнаружения CAPWAP
- Мульти-SSID с VLAN
- Поддержка ZyMesh
- Поддержка совместимых точек доступа
- Обнаружение чужих точек доступа

Широкополосный доступ по сотовой сети

- Резервное соединение WAN с помощью USB-модемов 3G и 4G*
- Автовозврат при восстановлении основного соединения WAN

Поддержка IPv6

- Двойной стек
- Туннелирование IPv4 (6rd and 6to4 transition tunnel)
- SLAAC, статичный IP-адрес
- DNS, DHCPv6 сервер/клиент
- Статическая маршрутизация и политики
- IPSec (IKEv2 6in6, 4in6, 6in4)

Соединение

- Режим маршрутизатора и/или моста
- Ethernet и PPPoE
- NAT и PAT
- Тегирование VLAN (802.1Q)
- Виртуальные интерфейсы (alias interface)
- Маршрутизация на базе политик (с учетом конкретного пользователя)
- NAT на базе политик (SNAT)
- GRE
- Динамическая маршрутизация (RIPv1/v2 и OSPF, BGP)
- DHCP клиент/сервер/ретранслятор
- Поддержка Dynamic DNS
- WAN-транки для 3 и более портов
- Ограничение сессий для отдельных хостов
- Гарантированная полоса пропускания
- Максимальная полоса пропускания
- Использование полосы пропускания с учетом приоритетов
- Ограничение полосы пропускания для отдельных пользователей
- Ограничение полосы пропускания для отдельных IP-адресов
- Управление полосой пропускания для сервисов/портов

Управление

Аутентификация

- Локальная база данных пользователей
- Внешняя база данных пользователей: Microsoft Windows Active Directory, RADIUS, LDAP
- Аутентификация IEEE 802.1x
- Аутентификация на web-портале
- Аутентификация XAUTH, IKEv2 и EAP VPN
- Привязка адресов IP-MAC
- Поддержка прозрачной авторизации (Single Sign-On)
- Поддержка 2-факторной аутентификации администраторов

Управление системой

- Ролевое администрирование
- Многоязычный web-интерфейс (HTTPS и HTTP)
- Интерфейс командной строки (консоль, web-консоль, SSH и telnet)
- SNMP v1, v2c, v3
- «Откат» к предыдущей конфигурации
- Обновление микропрограммы с использованием FTP, FTP-TLS и Web
- Оповещение о выходе новой версии микропрограммы и автоматическое обновление
- Два образа микропрограммы
- Cloud CNM SecuManager

Журналы событий и мониторинг

- Локальный журнал всех событий
- Поддержка Syslog (до 4 серверов)
- Предупреждения по электронной почте (до 2 серверов)
- Мониторинг трафика в реальном времени
- Встроенные ежедневные отчеты
- Cloud CNM SecuReporter

* Поддерживаемые USB-модемы 3G и 4G указаны в соответствующем списке продукта на web-сайте Zyxel.

Дополнительную информацию о продуктах можно найти на web-сайте www.zyxel.com