

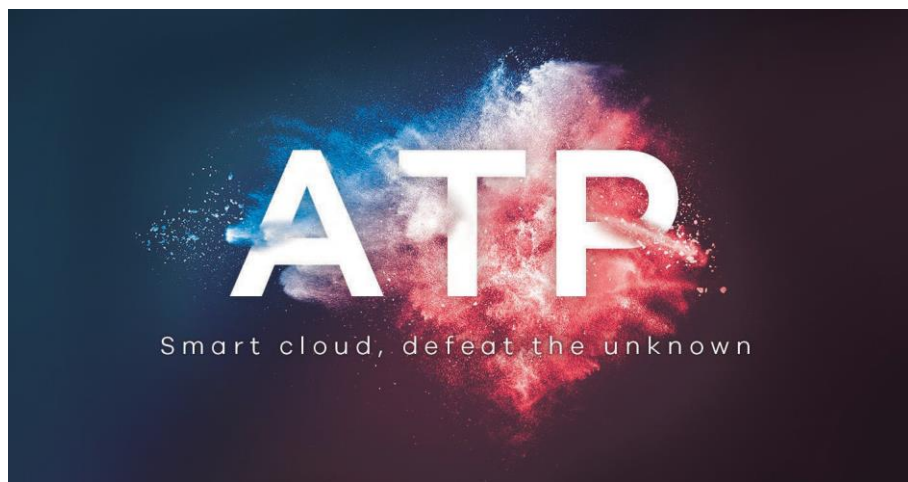


## ZyWALL ATP100/100W/200/500/700/800

### Межсетевой экран ATP

#### Межсетевой экран следующего поколения для SMB

Zyxel ZyWALL ATP – 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 Web-сайтов, патруль приложений, антивирус, репутационный фильтр, а также «песочницу», аналитический сервис SecuReporter и веб-интерфейс с инфографикой, представляя собой саморазвивающееся решение, обеспечивающее высокую производительность и эффективность защиты сети.



- 

Интеллектуальное обнаружение угроз с машинным обучением и глобальной базой данных об угрозах
- 

Песочница для защиты от неизвестных угроз
- 

Контентная фильтрация DNS- и URL-адресов обеспечивает высокую безопасность работы в интернете
- 

Надежная многоэшелонная защита
- 

CDR блокирует угрозы на границе сети
- 

Secure Wi-Fi гарантирует безопасность удаленной работы
- 

Отчеты и аналитика в облаке и на устройстве

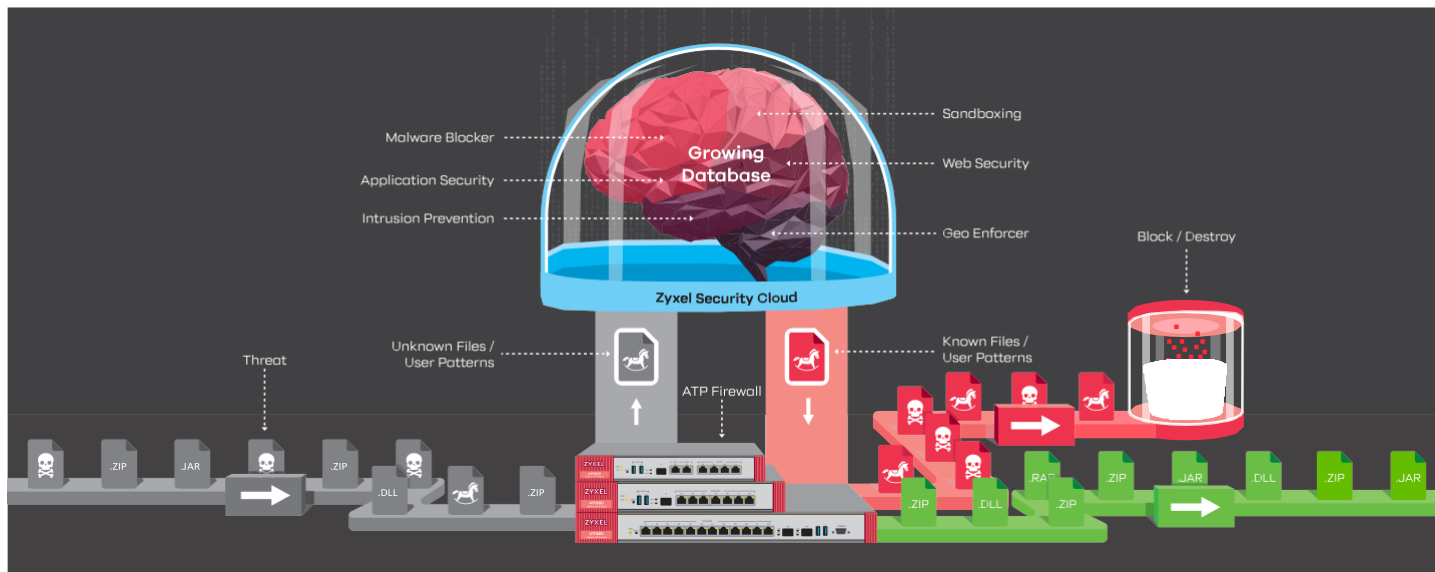
## Преимущества

### 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 интеллектуально 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

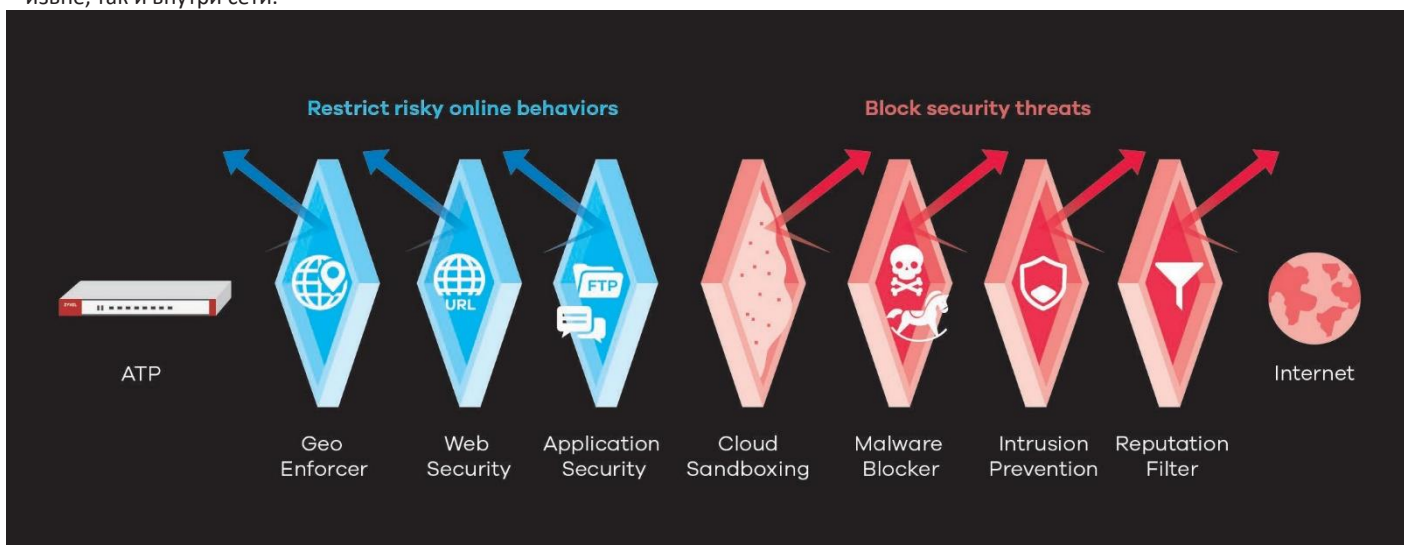
«Песочница» (Sandboxing) — это изолированная среда в облаке, в которой содержатся неизвестные файлы. Эти файлы не удается идентифицировать с помощью сервисов безопасности устройства, поэтому в песочнице эмулируется их поведение, чтобы определить, являются ли они опасными. Главное назначение песочницы — это инспекция поведения пакетов в изолированной среде, позволяющая выявить потенциальную угрозу до того, как она проникнет в сеть. Она позволяет идентифицировать новые типы угроз, которые не способны обнаружить традиционные статические механизмы защиты. Использование облачной песочницы в межсетевых экранах серии Zyxel ATP обеспечивает превентивную защиту от любых угроз нулевого дня (zero-day).



### Надежная многоэшелонная защита

Традиционные специализированные решения рассчитаны на отражение атак определенного типа, но вредоносный код постоянно совершенствуется и может проникнуть в сеть на любом этапе атаки, поэтому традиционные средства защиты оказываются неэффективными. В серии межсетевых экранов 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.



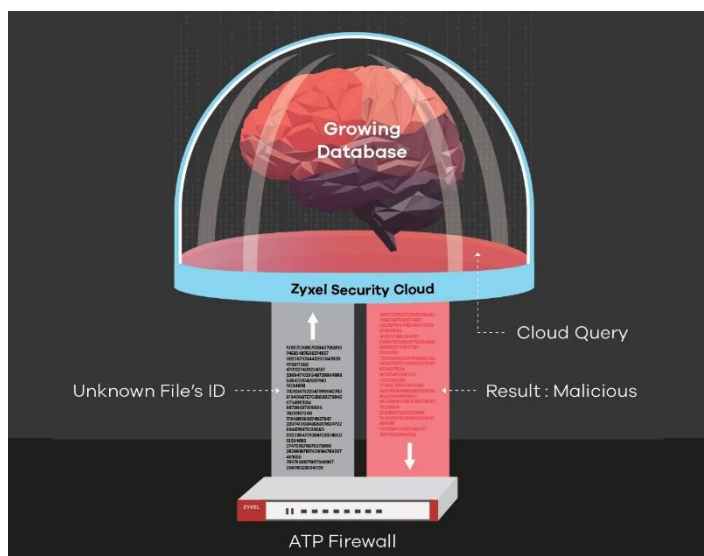
## Весь функционал сканирования веб-контента

Применяемые в межсетевых экранах ATP мощные фильтры веб-контента на основе репутации и категории обеспечивают высокую эффективность фильтрации и системы защиты. Динамическая классификация анализирует контент прежде неизвестных web-сайтов и доменов чтобы определить, не относится ли он к категории нежелательного, например, азартные и компьютерные игры, порнография и т.п. Новый функционал фильтра контента по DNS улучшает эффективность контроля доступа к web-сайтам, особенно к web-сайтам, использующим стандарт ESNI (Encrypted Server Name Indication), который шифрует адрес домена, к которому направляется запрос, из-за чего традиционный URL-фильтр не может идентифицировать такой домен.



## Гибридное сканирование, улучшающее эффективность блокировки вредоносного кода

Шлюз серии ATP не только применяет механизм потокового сканирования, который проверяет проходящие через шлюз файлы на вирусы и другие угрозы, но одновременно направляет запросы к базам данных в облаке безопасности Zyxel, в которые собирается информация из разных источников, и на ее основе с помощью машинного обучения и искусственного интеллекта выявляются новые ранее неизвестные угрозы. Гибридный режим защиты обеспечивает максимальную эффективность обнаружения угроз без снижения пропускной способности шлюза.



Техническая спецификация  
ZyWALL ATP100/100W/200/500/700/800

## Репутационный фильтр – превентивная защита на уровне IP/DNS/URL-адресов

Репутационный фильтр, включающий в себя фильтры репутаций IP-адресов, фильтр угроз DNS и фильтр угроз URL-адресов, проверяет IP-адреса/домены/URL-адреса по обновляемой в реальном времени облачной базе данных репутаций и на основе этой проверки определяет, можно ли доверять адресу или нет. Его применение улучшает эффективность блокировки доступа к опасным IP-адресам/доменам/URL-адресам, предотвращает доступ из скомпрометированных источников, обеспечивая гранулярную защиту от постоянно эволюционирующих киберугроз.



## Secure Wi-Fi гарантирует безопасность работы на удаленке

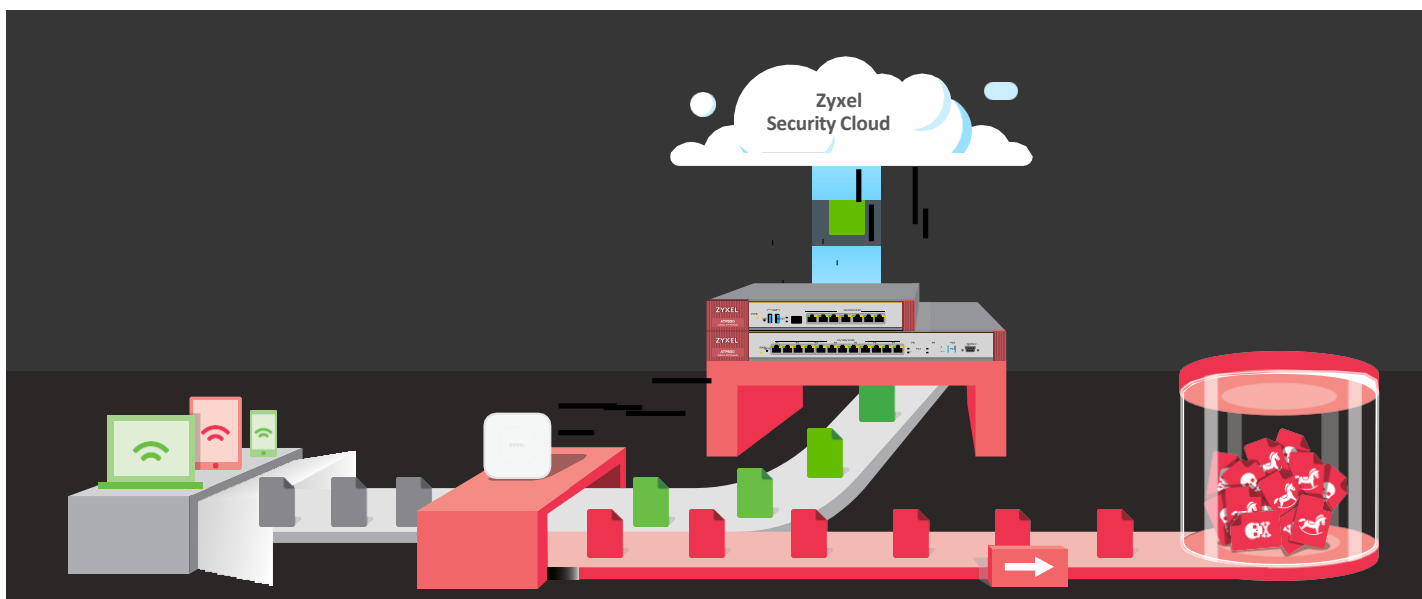
Из-за быстрого распространения мобильных устройств компаниям сегодня нужно найти правильный баланс между продуктивностью и безопасностью работы. Независимо от того, использует сотрудник, работающий из дома, проводное, беспроводное устройство или даже устройство «Интернета вещей» (IoT), сервис Secure Wi-Fi соединит его по защищенному туннелю L2 с офисом компании, и он сможет работать также удобно и безопасно, как если бы находился в офисе. Повышенная безопасность двухфакторной аутентификации улучшает продуктивность работы удаленного персонала и упрощает поддержку ИТ. Также сервис Secure Wi-Fi позволяет увеличить число управляемых точек доступа до максимума, поддерживаемого межсетевым экраном ATP.



## CDR блокирует угрозы до того, как они попали в сеть

Функция Совместное обнаружение и реагирование (CDR) идентифицирует угрозы в ваших бизнес-процессах, данных и пользователях и связанные с ними риски. В зависимости от периодичности акт и уровня угрозы она генерирует правила защиты.

Межсетевой экран ATP с помощью этих правил защиты автоматически блокирует угрозы уже на границе сети, радикально улучшая сетевую безопасность. Эта функция оптимально подходит для небольших компаний (SMB), использующих децентрализованную сетевую инфраструктуру на базе IoT.



## Аналитика и отчеты о неизвестных угрозах

Web-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 вывести список самых опасных web-сайтов, зараженных ботами, тип ботов и список внутренних хостов, которые контролируют эти боты. Аналитика репутации IP-адресов фильтра, фильтров DNS и URL отображает подробную информацию об IP/URL-адресах и доменах, которые были использованы для атак, и их степень риска.



## 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 конкретными потребностями.



CDR



Secure WiFi



Web Filtering



App Patrol



Email Security



Anti-Malware



IPS



Reputation Filter



Geo Enforcer



Sandboxing



SecuReporter




## Пакеты лицензий

Лицензируемый сервис	Функция	ZyWALL ATP100/100W/200/500/700/800*
		Gold (1 год/2 года/4 года)
Web Filtering	Контентная фильтрация	Да
App Patrol	Отслеживания и контроль работы приложений	Да
Email Security	Антиспам	Да
Anti-Malware	Антивирус с гибридным режимом	Да
	Интеллектуальное выявление угроз с применением машинного обучения	Да
IPS	Обнаружение и предотвращение вторжений	Да
Reputation Filter	Репутация IP-адресов	Да
	Фильтр угроз DNS	Да
	Фильтр угроз URL	Да
Geo Enforcer	Геополитики на основе IP-адресов	Да
Sandboxing	Песочница	Да
SecuReporter	SecuReporter Premium	Да
Secure Wi-Fi	Защищенный туннель для удаленных точек доступа	Да
	Сервис управления точками доступа* <sup>1</sup>	Максимальное число точек доступа
CDR	Совместное обнаружение и реагирование	Да




\*: Все модели ATP по умолчанию поставляются с лицензией Gold Security Pack на 1 год. Этот пакет лицензий нельзя передавать (non-transferable).

\*1: Gold Pack обеспечивает управление точками доступа в течение одного года (24 точки доступа для ATP100/100W, 40 точек доступа для ATP200, 72 точки доступа для ATP500, 264 точки доступа для ATP700 и 520 точек доступа для ATP800), по истечении лицензии можно управлять только 8 точками доступа

## Спецификации

Модель	ZyWALL ATP100	ZyWALL ATP100W	ZyWALL ATP200	
Фотография продукта				
<b>Спецификация оборудования</b>				
Порты	3 x LAN/DMZ, 1 x WAN, 1x OPT (LAN/WAN)	3 x LAN/DMZ, 1 x WAN, 1x OPT (LAN/WAN)	4 x LAN/DMZ, 2 x WAN, 1 x SFP (LAN/WAN)	
Порты USB 3.0	1	1	2	
Консольный порт	RJ-45	RJ-45	DB9	
Монтаж в стойке	-	-	Да	
Без вентилятора	Да	Да	Да	
<b>Емкость и производительность *1</b>				
Пропускная способность межсетевого экрана SPI (Мбит/сек)*2	1 000	1 000	2 000	
Пропускная способность VPN (Мбит/сек)*3	300	300	500	
Пропускная способность IDP (Мбит/сек)*4	600	600	1 200	
Пропускная способность AV (Мбит/сек)*4	380	380	630	
Пропускная способность UTM (AV и IDP) (Мбит/сек)*4	380	380	600	
Максимальное число одновременных сессий TCP*5	300 000	300 000	600 000	
Максимальное число туннелей IPsec VPN*6	40	40	100	
Рекомендуемое число туннелей IPsec шлюз-шлюз	20	20	50	
Максимальное число SSL VPN	30	30	60	
Количество интерфейсов VLAN	8	8	16	
<b>Производительность в Speedtest на одном гигабитном канале</b>				
Пропуск. способность межсетевого экрана SPI (Мбит/сек)*7	850	850	900	
<b>Основные функции</b>				
Сервисы безопасности	Sandboxing*8	Да	Да	Да
	Web Filtering*8	Да	Да	Да
	Application Patrol*8	Да	Да	Да
	Anti-Malware*8	Да	Да	Да
	IPS*8	Да	Да	Да
	Reputation Filter*8	Да	Да	Да
	Geo Enforcer*8	Да	Да	Да
	SecuReporter Premium*8	Да	Да	Да
	Collaborative Detection& Response*8	Да	Да	Да
	SSL (HTTPS) инспекция	Да	Да	Да
2-факторная аутентификация	Да	Да	Да	
Функции VPN	VPN	IKEv2, IPsec, SSL, L2TP/IPsec	IKEv2, IPsec, SSL, L2TP/IPsec	IKEv2, IPsec, SSL, L2TP/IPsec
	Microsoft Azure	Да	Да	Да
	Amazon VPC	Да	Да	Да

Модель		ZyWALL ATP100	ZyWALL ATP100W	ZyWALL ATP200
<b>Основные функции</b>				
Управление WLAN	Число управляемых точек доступа по умолчанию	8	8	8
	Рекомендуемое максимальное число точек в одной группе	10	10	20
	Сервис Secure WiFi*8	Да	Да	Да
	Максимальное число туннельных точек доступа	6	6	10
	Максимальное число управляемых точек доступа	24	24	40
Управление соединениями	Device HA Pro	-	-	-
	Link Aggregation (LAG)	-	-	-
<b>Требования к питанию</b>				
Источник питания		12 В постоянного тока, максимум 2 А	12 В постоянного тока, максимум 2 А	12 В постоянного тока, максимум 2.5 А
Максимальное энергопотребление (Ватт)		12.5	12.5	13.3
Тепловыделение (BTU/час)		42.65	42.65	45.38
<b>Физические характеристики</b>				
Без упаковки	Размеры (ШxГxВ) (мм):	216 x 147.3 x 33	216 x 147.3 x 33	272 x 187 x 36
	Вес (кг)	0.85	0.85	1.4
В упаковке	Размеры (ШxГxВ) (мм):	284 x 190 x 100	284 x 190 x 100	427 x 247 x 73
	Вес (кг)	1.4	1.4	2.42
Аксессуары в комплекте поставки		<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Кабель RJ-45</li> <li>• Кабель RS-232</li> </ul>	<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Кабель RJ-45</li> <li>• Кабель RS-232</li> </ul>	<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Набор для монтажа в стойке</li> </ul>
<b>Требования к окружающей среде</b>				
Эксплуатация	Температура	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)
Хранение	Температура	-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)
MTBF (часов)		989 810.8	989 810.8	529 688.2
Акустический шум		-	-	-
<b>Сертификаты</b>				
EMC		FCC Part 15 (Class B), CE EMC (Class B), BSMI	FCC Part 15 (Class B), CE EMC (Class B), BSMI	FCC Part 15 (Class B), CE (Class B), C-Tick (Class B), BSMI
Safety		LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

Модель	ZyWALL ATP500	ZyWALL ATP700	ZyWALL ATP800	
Фотография продукта				
<b>Спецификация оборудования</b>				
Порты	7 (конфигурируемые), 1x SFP (конфигурируемый)	12 (конфигурируемые), 2x SFP (конфигурируемые)	12 (конфигурируемые), 2x SFP (конфигурируемые)	
Порты USB 3.0	2	2	2	
Консольный порт	DB9	DB9	DB9	
Монтаж в стойке	Да	Да	Да	
Без вентилятора	-	-	-	
<b>Емкость и производительность *1</b>				
Пропускная способность межсетевое экрана SPI (Мбит/сек)*2	2,600	6,000	8,000	
Пропускная способность VPN (Мбит/сек)*3	900	1 200	1 500	
Пропускная способность IPS (Мбит/сек)*4	1 700	2 200	2 700	
Пропускная способность антивируса (Мбит/сек)*4	900	1 600	2 000	
Пропускная способность UTM (AV и IDP) (Мбит/сек)*4	890	1 500	1 900	
Максимальное число одновременных сессий TCP*5	1 000 000	1 600 000	2 000 000	
Максимальное число туннелей IPsec VPN*6	300	1 000	1 000	
Рекомендуемое число туннелей IPsec VPN между шлюзами	150	300	300	
Максимальное число SSL VPN	150	150	500	
Количество интерфейсов VLAN	64	128	128	
<b>Производительность в Speedtest на одном гигабитном канале</b>				
Пропуск. способность межсетевое экрана SPI (Мбит/сек)*7	900	930	930	
<b>Управление WLAN</b>				
Сервисы безопасности	Sandboxing*8	Да	Да	Да
	Web Filtering*8	Да	Да	Да
	Application Patrol*8	Да	Да	Да
	Anti-Malware*8	Да	Да	Да
	IPS*8	Да	Да	Да
	Reputation Filter*8	Да	Да	Да
	Geo Enforcer*8	Да	Да	Да
	SecuReporter Premium*8	Да	Да	Да
	Collaborative Detection & Response*8	Да	Да	Да
	SSL (HTTPS) инспекция	Да	Да	Да
2-факторная аутентификация	Да	Да	Да	
Функция VPN	VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
	Microsoft Azure	Да	Да	Да
	Amazon VPC	Да	Да	Да



Модель		ZyWALL ATP500	ZyWALL ATP700	ZyWALL ATP800
<b>Основные функции</b>				
Управление WLAN	Число управляемых точек доступа по умолчанию	8	8	8
	Рекомендуемое максимальное число точек в одной группе	60	200	300
	Сервис Secure WiFi*8	Да	Да	Да
	Максимальное число туннельных точек доступа	18	66	130
	Максимальное число управляемых точек доступа	72	264	520
Управление соединениями	Device HA Pro	Да	Да	Да
	Link Aggregation (LAG)	Да	Да	Да
<b>Требования к питанию</b>				
Источник питания	12 В постоянного тока, максимум 4.7 А	100-240 В переменного тока, 50/60 Гц, максимум 2.5 А	100-240 В переменного тока, 50/60 Гц, максимум 2.5 А	
Максимальное энергопотребление (Ватт)	24.1	46	46	
Тепловыделение (BTU/час)	82.23	120.1	120.1	
<b>Физические характеристики</b>				
Без упаковки	Размеры (ШxГxВ) (мм):	300 x 188 x 44	430 x 250 x 44	430 x 250 x 44
	Вес (кг)	1.65	3.3	3.3
В упаковке	Размеры (ШxГxВ) (мм):	351 x 152 x 245	519 x 392 x 163	519 x 392 x 163
	Вес (кг)	2.83	4.8	4.8
Аксессуары в комплекте поставки	<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Силовой кабель</li> <li>• Набор для монтажа в стойке</li> </ul>	<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Набор для монтажа в стойке</li> </ul>	<ul style="list-style-type: none"> <li>• Адаптер питания</li> <li>• Набор для монтажа в стойке</li> </ul>	
<b>Требования к окружающей среде</b>				
Эксплуатация	Температура	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)
Хранение	Температура	-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)
MTBF (часов)	529 688.2	947 736	947 736	
Акустический шум	24.5 дБА при работе при температуре до +25°C, 41.5 дБА при максимальной скорости вращения вентилятора.	25.3 дБА при работе при температуре до +25°C, 46.2 дБА при максимальной скорости вращения вентилятора.	25.3 дБА при работе при температуре до +25°C, 46.2 дБА при максимальной скорости вращения вентилятора.	
<b>Сертификаты</b>				
EMC	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	
Безопасность	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	

\*: Эта таблица для микропрограммы ZLD5.00 и более поздней версии.

\*1: На практике производительность может быть меньше из-за конфигурации системы, 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 AV (в режиме Express) 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: Включая туннели между шлюзами и с клиентами.

\*7: Тесты Speedtest проводились с использованием одного канала 1 Гбит/сек в реальной сети, и на их результаты могло повлиять качество канала сервис-провайдера.

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

## Спецификация беспроводного интерфейса

Модель		ZyWALL ATP100W
Соответствие стандартам беспроводных сетей		802.11 a/b/g/n/ac
Частота беспроводной сети		2.4 / 5 ГГц
Количество радиомодулей		2
Количество SSID		8
Максимальная мощность передатчика	США (FCC) 2.4 ГГц	25 дБм, 3 антенны
	США (FCC) 5 ГГц	25 дБм, 3 антенны
	Европа (ETSI) 2.4 ГГц	20 дБм, 3 антенны
	Европа (ETSI) 5 ГГц	20 дБм, 3 антенны
Количество антенн		3 съемные антенны
Усиление антенн		2 дБи для частоты 2.4 ГГц 3 дБи для частоты 5 ГГц
Скорость передачи данных		802.11n: до 450 Мбит/сек 802.11ac: до 1300 Мбит/сек
Частотный диапазон	2.4 ГГц (IEEE 802.11 b/g/n)	США (FCC): 2.412 - 2.462 ГГц Европа (ETSI): 2.412 - 2.472 ГГц Тайвань (NCC): 2.412 - 2.462 ГГц
	5 ГГц (IEEE 802.11 a/n/ac)	США (FCC): 5.150 - 5.250 ГГц; 5.250 - 5.350 ГГц; 5.470 - 5.725 ГГц; 5.725 - 5.850 ГГц Европа (ETSI): 5.15 - 5.35 ГГц; 5.470 - 5.725 ГГц Тайвань (NCC) :5.15 - 5.25 ГГц; 5.25 - 5.35 ГГц; 5.470 - 5.725 ГГц; 5.725 - 5.850 ГГц
Чувствительность приемника	2.4 ГГц	11 Мбит/сек ≤ -87 дБм 54 Мбит/сек ≤ -77 дБм HT20 ≤ -71 дБм HT40 ≤ -68 дБм
	5 ГГц	54 Мбит/сек ≤ -74 дБм HT40, MCS23 ≤ -68 дБм VHT40, MCS9 ≤ -62 дБм HT20, MCS23 ≤ -71 дБм VHT20, MCS8 ≤ -66 дБм VHT80, MCS9 ≤ -59 дБм

## 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/N.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

- Поточковый механизм сканирования (режим Stream)
- Поддержка протоколов HTTP, FTP, SMTP и POP3
- Отсутствие ограничений на размер файла
- Автоматическое обновление сигнатур

#### Гибридный режим сканирования на вирусы

- Одновременное потоковое сканирование и запросы в облако
- Использует локальный кэш и постоянно растущую базу данных с 30+ миллиардов сигнатур
- Поддержка протоколов на базе HTTP, HTTPS и FTP
- Поддержка различных типов файлов

## Антиспам

- Прозрачный перехват почты с использованием протоколов SMTP и POP3
- Обнаружение в почте спама и фишинга
- Черный и белый список адресов
- Поддержка проверки DNSBL

## Репутационный фильтр IP-адресов

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

## Фильтр угроз DNS

- Блокирует доступ клиентов к опасным доменам
- Эффективная защита при использовании любого протокола IP-сетей

## Фильтр угроз URL

- Блокировка web-сайтов ботнета C&C
- Блокировка опасных URL-адресов
- Поддержка внешних черных списков URL-адресов

## Контентная фильтрация

- Фильтр доменов HTTPS
- Поддержка SafeSearch (безопасный поиск)
- Применение белого списка web-сайтов
- Черный и белый список URL-адресов, блокировка по ключевым словам
- Настраиваемые предупреждения и URL-перенаправление
- Настраиваемая страница блокировки контента
- Число категорий URL-адресов увеличено до 111
- Поддержка CTIRU (Counter-Terrorism Internet Referral Unit)

## 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 сканирования для антивируса (включая песочницу), IDP, репутации IP-адресов и фильтра угроз URL-адресов

## Совместное обнаруж. и реагирование

- Выдача предупреждений/

Техническая спецификация

ZyWALL ATP100/100W/200/500/700/800

блокировка/перемещение в карантин

- Блокировка доступа к сети опасных беспроводных клиентов
- Настраиваемые предупреждения и перенаправление по URL-адресу
- Список IP-адресов или MAC-адресов, для которых не выполняется проверка

## VPN

### IPSec VPN

- Управление ключами: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Шифрование: DES, 3DES, AES (256-bit)
- Аутентификация: MD5, SHA1, SHA2 (512-bit)
- Поддержка PFS (DH группы) 1, 2, 5, 14, 15-18, 20-21
- 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

### Secure Wi-Fi

- Защищенный туннель для удаленных точек доступа
- Доступ из дома по L2 к офису (защищенный туннель)
- 2-факторная аутентификация с использованием Google Authenticator
- Поддержка WPA2 Enterprise (802.1x)
- Контроль штормов
- Можно применять как в режиме локального управления точкой доступа, так и управления из Nebula (когда ATP получит поддержку Nebula)

### Контроллер WLAN

- Поддержка контроллера точек доступа
- Поддержка точек доступа 802.11ax Wi-Fi 6 и WPA3
- Поддержка 802.11k/v/r
- L2 изоляция

- Поддержка автоматического обновления микропрограмм точек доступа
- Включение Wi-Fi по расписанию
- Динамический выбор каналов (DCS)
- Приоритезация диапазона 5 ГГц и предотвращение «залипания» клиентов
- 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\*2
- 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
- Балансировка нагрузки NAT для локальных серверов
- 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 приложений
- Поддержка Link Aggregation\*1

## 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 с EAP VPN
- Привязка адресов IP-МАС
- Поддержка 2-факторной аутентификации администраторов с использованием Google Authenticator как второго фактора

#### 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
- Автоматическое резервное копирование конфигурации
- Обновление микропрограммы с использованием FTP, FTP-TLS и Web-интерфейса
- 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.

\*1: поддерживают модели ATP500/700/800.

## Список совместимых точек доступа

### Поддержка Secure Wi-Fi

Серия	Модель	Максимальное число туннельных точек доступа	Поддерживаемые туннельные точки доступа
ATP	ATP100(W)	6	<ul style="list-style-type: none"> <li>• WAX650S</li> <li>• WAX610D</li> <li>• WAX510D</li> <li>• WAC500</li> <li>• WAC500H</li> </ul>
	ATP200	10	
	ATP500	18	
	ATP700	66	
	ATP800	130	
USG FLEX	USG FLEX 100(W)	6	
	USG FLEX 200	10	
	USG FLEX 500	18	
	USG FLEX 700	66	
VPN	VPN50	10	
	VPN100	18	
	VPN300	66	
	VPN1000	258	

### Сервисы управления точками доступа

Продукт	Точки доступа Unified	Точки доступа Unified Pro	
<b>Модели</b>	<ul style="list-style-type: none"> <li>• NWA5301-NJ</li> <li>• NWA5121-NI</li> <li>• NWA5123-AC HD</li> <li>• NWA5123-AC</li> <li>• NWA5123-NI</li> </ul>	<ul style="list-style-type: none"> <li>• WAC5302D-S</li> <li>• WAX510D</li> <li>• WAC5302D-Sv2*</li> <li>• WAC500*</li> <li>• WAC500H*</li> </ul>	<ul style="list-style-type: none"> <li>• WAC6103D-I</li> <li>• WAC6503D-S</li> <li>• WAC6502D-S</li> <li>• WAC6303D-S</li> <li>• WAC6553D-E</li> </ul>
<b>Функции</b>			
<b>Централизованное управление</b>	Да	Да	
<b>Автоматическая настройка</b>	Да	Да	
<b>Передача данных</b>	Локальная	Локальная/туннельная	
<b>ZyMesh</b>	Да	Да	

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

## Аксессуары

### Трансиверы (опция)

Модель	Скорость передачи данных	Коннектор	Длина волны	Максимальное расстояние	Тип оптики	DDMI
SFP10G-SR*	10-Gigabit SFP+	Duplex LC	850 нм	300 м	Мультимод	Да
SFP10G-SR-E*	10-Gigabit SFP+	LC	850 нм	300 м	Мультимод	Да
SFP10G-LR*	10-Gigabit SFP+	Duplex LC	1310 нм	10 км	Одномод	Да
SFP10G-LR-E*	10-Gigabit SFP+	LC	1310 нм	10 км	Одномод	Да
SFP-1000T	Gigabit	RJ-45	-	100 м	Мультимод	-
SFP-SX-D	Gigabit	LC	850 нм	550 м	Мультимод	Да
SFP-SX-E	Gigabit	LC	850 нм	550 м	Мультимод	Да
SFP-LX-10-D	Gigabit	LC	1310 нм	10 км	Одномод	Да
SFP-LX-10-E	Gigabit	LC	1310 нм	10 км	Одномод	Да
SFP-LHX1310-40-D	Gigabit	LC	1310 нм	40 км	Одномод	Да
SFP-ZX-80-D	Gigabit	LC	1550 нм	80 км	Одномод	Да
SFP-BX1310-10-D* <sup>1</sup>	Gigabit	LC	1310 нм (TX) 1490 нм (RX)	10 км	Одномод	Да
SFP-BX1310-E* <sup>1</sup>	Gigabit	LC	1310 нм (TX) 1550 нм (RX)	20 км	Одномод	Да
SFP-BX1490-10-D* <sup>1</sup>	Gigabit	LC	1490 нм (TX) 1310 нм (RX)	10 км	Одномод	Да
SFP-BX1550-E* <sup>1</sup>	Gigabit	LC/SC	1550 нм (TX) 1310 нм (RX)	20 км	Одномод	Да

\*: Скорость 10-Gigabit SFP+ поддерживает только серия USG2200-VPN.

\*1: Трансиверы SFP-BX1310-10-D и SFP-BX1490-10-D, SFP-BX1310-E и SFP-BX1550-E должны использоваться парами.

Дополнительную информацию о продуктах можно найти на нашем web-сайте [www.zyxel.com](http://www.zyxel.com)  
Copyright © 2021 Zyxel и/или ее дочерние компании. Все права защищены.  
Все спецификации могут быть изменены без письменного уведомления.



05/05/21