



ZyWALL USG40/40W/60/60W

Унифицированный шлюз безопасности

Цифровые технологии радикально упростили многие аспекты нашей жизни, но у них есть и обратная сторона. Новые возможности для работы и взаимодействия создают и новые проблемы для малого бизнеса, в том числе контроль над подключенными к сети различными смарт-устройствами, число которых постоянно увеличивается, назначение повышенного приоритета одним облачным приложениям, которые необходимы для работы, и блокировка других облачных приложений, защита от происходящих каждый день кибератак и попыток проникновения через Web. Угрозы становятся все более опасными, а проблемы усложняются, поэтому небольшим компаниям с ограниченными ИТ-ресурсами трудно контролировать ситуацию.

ZyWALL USG40/40W/60/60W – это межсетевые экраны UTM «всё-в-одном», специально разработанные для обеспечения безопасности сетей небольших компаний и использующих все функции UTM, в том числе защита от вирусов, регулирование использования приложений и контроль трафика. Встроенная точка доступа (модели USG40W и USG60W) и контроллер беспроводной сети позволяют сразу же развернуть хот-спот беспроводной сети и легко масштабировать его по мере необходимости. Продукты серии ZyXel USG поддерживают VPN, что позволяет небольшим компаниям организовать безопасную связь со своими партнерами, а филиалам – с главными офисами. В эти продукты интегрированы весь функционал, который может понадобиться малому бизнесу, поэтому они обеспечивают легкое централизованное управление с низкой совокупной стоимостью владения (TCO).



Межсетевой экран UTM «всё-в-одном» для малого бизнеса



Комплексная защита сети с антивирусом, антиспамом, контентной фильтрацией, обнаружением и предотвращением вторжений и патрулем приложений



Надежная защита с помощью SSL, IPSec и L2TP over IPSec соединений VPN



Унифицированные политики безопасности



Встроенная беспроводная точка доступа с одним (USG40W) либо двумя (USG60W) радиомодулями



Облачный сервис интеллектуальной аналитики и подготовки отчетов SecuReporter



Преимущества

Гарантированная безопасность

ZyWALL USG40/40W/60/60W – это межсетевые экраны UTM, которые обеспечивают безопасность корпоративного уровня и доступны по цене для небольших компаний. Они реализуют многоуровневую защиту сети и эффективный контроль использования Web-приложений (например, Facebook, Google Apps и Netflix) с применением таких механизмов защиты от вредоносного кода, как межсетевой экран, антивирус, антиспам, контентная фильтрация, обнаружение и предотвращение вторжений и патруль приложений. Также для контентной фильтрации реализована блокировка по географическому расположению IP-адреса, что еще больше повышает эффективность обнаружения угроз. Теперь небольшие компании надежно защищены от киберугроз и могут блокировать снижающие продуктивность работы персонала спам и доступ к социальным сетям.

Wi-Fi везде, где он нужен

Учитывая растущую популярность использования клиентских устройств по принципу BYOD, шлюзы ZyWALL USG помогают малому бизнесу удовлетворить потребность в Wi-Fi по мере необходимости. Модели USG40W и USG60W оборудованы встроенной беспроводной точкой доступа с одним и двумя радиомодулями, поэтому они обеспечат развертывание Wi-Fi в небольшом офисе сразу после первого включения устройства. Интегрированный контроллер беспроводной сети с технологией Zyxel AP Controller позволяет централизованно управлять до 18 точками доступа. С помощью шлюзов Zyxel USG можно при необходимости легко развернуть Wi-Fi в нескольких зонах, например, на входе и в переговорных комнатах.

Быстрое и безопасное обновление микропрограммы

Поиск последних обновлений микропрограммы, не говоря уже о выборе ее версии для конкретной модели устройства и инсталляции, часто превращается в длительную и сложную процедуру. Встроенный в межсетевые экраны Zyxel USG сервис Cloud Helper существенно упрощает решение этих задач. С помощью простых операций этот сервис помогает пользователю получить последнюю информацию о микропрограмме, поэтому новейшая версия становится доступна сразу после размещения в нашей официальной базе данных, что гарантирует ее аутентичность и надежность.

Полный контроль

SecuReporter – это облачный сервис интеллектуальной аналитики и подготовки отчетов с функциями сбора и корреляции данных. Вместе с USG предоставляет лицензия на использование сервиса SecuReporter в течение 1 года, обеспечивающая сохранение логов за 7 дней и применение визуальной аналитики. SecuReporter обеспечивает анализ тенденций всех угроз (Threat Trend), спама, категорий небезопасных web-сайтов, самых часто возникающих угроз (вирусы, IDP, спам) и поведения пользователей, предоставляя специалистам по информационной безопасности подробные сведения об угрозах.

Упрощенная процедура управления

Управление многочисленными параметрами сложной конфигурации обычно требует больших затрат рабочего времени. Шлюзы Zyxel USG поддерживают упрощенный режим настройки “Easy Mode” в Web-интерфейсе, рассчитанный на небольшие фирмы и пользователей из сектора SOHO. В Easy Mode настройка выполняется с помощью пиктограмм и удобной веб-консоли, упрощающих управление и мониторинг состояния межсетевого шлюза. Параметры настройки приложений и функций также настраиваются с помощью встроенных программ-мастеров. Режим Easy Mode помогает пользователям Zyxel USG, установленных в небольших фирмах и SOHO, с минимальными усилиями получить все преимущества высокоскоростных и безопасных сетей.

Преимущества Zyxel One Network

Избавляя заказчиков от необходимости выполнения рутинных операций развертывания и управления сетью, утилита Zyxel One Network (ZON) упрощает конфигурирование, управление и устранение сбоев, что позволяет нашим клиентам больше времени уделять своему основному бизнесу. Технология Zyxel Smart Connect помогает сетевому оборудованию Zyxel идентифицировать в сети другие устройства Zyxel, что дополнительно облегчает управление сетью, позволяя одним щелчком мыши дистанционно выполнять сброс в заводские настройки или перезагрузку устройства. Zyxel One Network обеспечивает интеграцию различного подключенного к сети оборудования, начиная с коммутаторов и заканчивая беспроводными точками доступа и шлюзами.

Сравнительная таблица устройств серии ZyWALL USG



Модель	USG40 /40W	USG60 /60W	USG110	USG210	USG310	USG1100	USG1900	USG2200
Описание	Малый бизнес		SMB			MB		
Пропускная способность межсетевое экрана (Мбит/сек)	400	1 000	1 600	1 900	5 000	6 000	7 000	25 000
Максимальное число одновременных сессий	50 000	100 000	150 000	200 000	500 000	1 000 000	1 000 000	1 500 000
Пропускная способность UTM (AV и IDP) (Мбит/сек)	50	90	450	500	550	650	710	1 000
Пропускная способность IDP (Мбит/сек)	95	150	590	660	900	1000	1200	2 000
Пропускная способность AV (Мбит/сек)	50	90	450	500	550	650	710	1 000
Amazon VPC ^{*1}	Да	Да	Да	Да	Да	Да	Да	Да
Microsoft Azure	Да	Да	Да	Да	Да	Да	Да	Да
Cloud CNM	Да	Да	Да	Да	Да	Да	Да	Да
SecuReporter ^{*2}	Да	Да	Да	Да	Да	Да	Да	Да
Управление хот-спотами ^{*2}	-	Да	Да	Да	Да	Да	Да	Да
Device HA Pro	-	-	Да	Да	Да	Да	Да	Да

*1: Для ZyWALL/USG доступна настройка при помощи интерфейса командной строки CLI

*2: Для использования этой функции и расширения ее емкости нужна лицензия на сервис Zyxel

Сервисы и лицензии

ZyWALL USG40/40W/60/60W 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.

*: Управление хот-спотами поддерживает только USG60/60W с микропрограммой ZLD версии 4.35 или более поздней.



Антивирус



Антиспам



Обнаружение и предотвращение вторжений



Патруль приложений



Контент. фильтрация



SecuReporter



Контроллер точек доступа



Управление хот-спотами

Основные преимущества

Два интерфейса WAN и широкополосный доступ по сотовой сети

У шлюзов ZyWALL USG два интерфейса WAN и поддержка широкополосного доступа к Интернету по сотовой сети, поэтому они обеспечивают непрерывный доступ к Интернету. Два порта Ethernet, которые используются для подключения к WAN, можно объединять по схеме active-active для балансировки нагрузки, либо active-passive для переключения при отказе основной линии на резервную (failover). Также в качестве резервного канала WAN можно использовать широкополосное подключение к сотовой сети с помощью USB-модема.

Унифицированная политика безопасности

Унифицированная политика безопасности реализует управление и конфигурацию на базе объектов всех политик, связанных с безопасностью. Пользователи могут легко применять все критерии политики к любой функции UTM и в результате гораздо быстрее настраивать устройство.

Cloud Helper

Cloud Helper максимально упрощает обновление микропрограммы, поэтому пользователю не надо отслеживать выпуск ее новой версии и искать файлы для загрузки обновлений. При использовании этого сервиса весь процесс загрузки и обновления микропрограммы сокращается до несколько простых операций.

Утилита Zyxel One Network

Интеллектуальные функции утилиты ZON позволяют сетевому администратору обновлять микропрограммы сразу на группе устройств, удаленно перезагружать такие устройства, как потолочные точки доступа, либо одним щелчком запускать интерфейс устройства для настроек его конфигурации. С помощью этой утилиты можно легко выполнять сложные операции управления различным оборудованием, в том числе точками доступа, коммутаторами и шлюзами.

Отсутствие вентилятора

В ZyWALL USG нет встроенного вентилятора, поэтому в корпус устройства проникает меньше пыли, из-за которой оно может выйти из строя. Также благодаря отсутствию вентилятора ZyWALL USG работает практически бесшумно, поэтому этот шлюз с низким тепловыделением можно установить в небольшом офисе рядом с рабочими местами персонала.

Easy Mode

Пользовательский интерфейс ZyWALL USG позволяет легко и с минимальными затратами рабочего времени подготовить устройство к работе и менять его конфигурацию для обеспечения высокоскоростного и безопасного подключения к Интернету. Интегрированные программы-мастера помогают быстро запустить самые часто используемые приложения и функции.

Надежная защита соединений VPN

ZyWALL USG поддерживает высокопроизводительные протоколы IPSec, L2TP over IPSec и SSL VPN для разных сценариев построения соединений VPN между площадками и между площадкой и клиентами. Применение этих протоколов вместе с надежной аутентификацией SHA-2 позволяет с помощью ZyWALL USG обеспечить максимальную безопасность VPN для передачи важной для бизнеса информации.

Интегрированный контроллер беспроводной сети

Интегрированный контроллер беспроводной сети поддерживает CAPWAP и обеспечивает централизованную авторизацию и управление доступом для нескольких точек доступа, подключенных к сети. По умолчанию ZyWALL USG40/40W/60/60W могут управлять 2 точками доступа, а при покупке лицензии - до 18 точками доступа.

Встроенная беспроводная точка доступа

Оборудованные беспроводной точкой доступа с одним или двумя радиомодулями шлюзы ZyWALL USG40W и USG60W великолепно подходят для розничной торговли и офиса. Модель USG60W поддерживают технологию 802.11 a/b/g/n и обеспечивают работу Wi-Fi как в диапазоне 2.4 ГГц, так и 5 ГГц.

Соответствие стандарту PCI DSS

Zyxel USG соответствует международному стандарту безопасности данных платежных карт Payment Card Industry Data Security Standard (PCI DSS), требования которого должны соблюдать компании во многих секторах экономики. Спецификация PCI DSS определяет требования к продавцам, эмитентам платежных карт, процессинговым центрам и поставщикам сервисов, участвующим в процесс обработки транзакций с применением платежных карт, включая обработку данных о держателе платежной карты, их передачу и хранение.

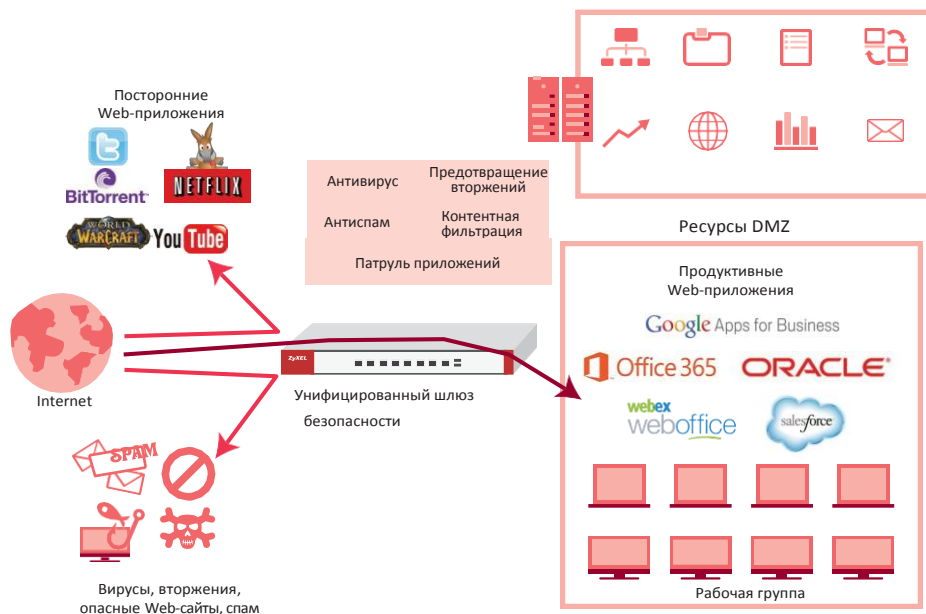
Аналитика состояния безопасности с отчетами

SecuReporter – это пакет утилит аналитики и подготовки отчетов, обеспечивающий идентификацию сетевых угроз и графическое представление результатов работы сервисов безопасности, статистики инцидентов безопасности, использования приложений, посещений web-сайтов и переданного трафика, а также состояния устройства. Также с помощью SecuReporter можно подготавливать отчеты по требованию, либо по расписанию (раз в день/неделю/месяц).

Сценарии применения

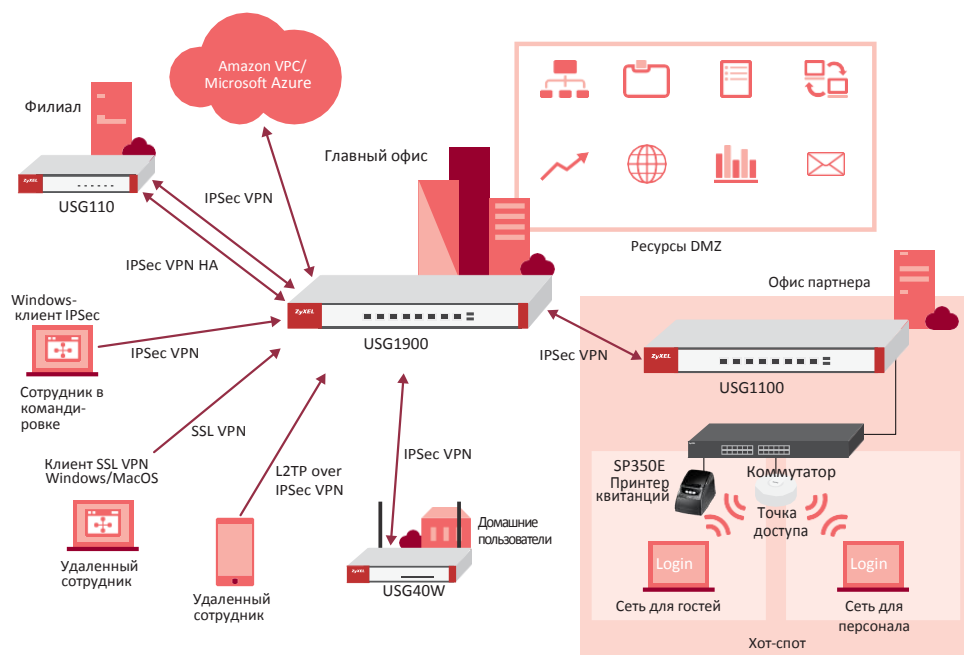
Защита от вирусов и оптимизация использования приложений

- С помощью антивируса, антиспама и предотвращения вторжений обеспечивается надежная многоуровневая защита сети компании от различного вредоносного кода
- Контентная фильтрация блокирует доступ к опасным и не имеющим отношения к бизнесу компании Web-сайтам
- Патруль приложений не только блокирует или ограничивает доступ к посторонним Web-приложениям, но и улучшает производительность продуктивных Web-приложений



Использование VPN





- Филиалы, партнеры и домашние пользователи с помощью межсетевых экранов ZyWALL организуют соединение IPSec VPN между площадками
- Филиалы могут дополнительно использовать IPSec VPN HA (балансировка нагрузки и переключение при отказах) для высокой доступности соединения VPN
- Удаленные пользователи получают безопасный доступ к корпоративным ресурсам со своих компьютеров и смартфонов по VPN с применением SSL, IPSec и L2TP over IPSec
- Установленные в главном офисе межсетевые экраны ZyWALL USG для соединения IPSec VPN с Amazon VPC/Microsoft Azure обеспечивают безопасный доступ к развернутым в облаке приложениям.



Управление хот-спотами

- Высокоскоростной доступ к Интернету
- Уровни качества сервиса
- Сохранение истории операций в соответствии с требованиями законодательства
- Эффективный контроль безопасности
- Разные варианты контроля доступа к сети (бесплатный либо платный доступ, вход по учетной записи социальной сети)

Спецификации

Модель	USG40	USG40W	USG60	USG60W
Фотография продукта				
				
Спецификация оборудования				
Интерфейсы	3 x LAN/DMZ, 1 x WAN, 1 x OPT	3 x LAN/DMZ, 1 x WAN, 1 x OPT	4 x LAN/DMZ, 2 x WAN	4 x LAN/DMZ, 2 x WAN
USB-порты	1	1	2	2
Консольный порт	Да (RJ-45)	Да (RJ-45)	Да (DB9)	Да (DB9)
Монтаж в стойке	-	-	Да	Да
Без вентилятора	Да	Да	Да	Да
Емкость и производительность *1				
Пропускная способность межсетевого экрана SPI (Мбит/сек) *2	400	400	1000	1000
Пропускная способность VPN (Мбит/сек) *3	100	100	180	180
Пропускная способность IDP (Мбит/сек) *4	95	95	150	150
Пропускная способность AV (Мбит/сек) *4	50	50	90	90
Пропускная способность UTM (AV и IDP) *4	50	50	90	90
Максимальное число одновременных сессий TCP *5	50 000	50 000	100 000	100 000
Макс. число туннелей IPSec VPN *6	20	20	40	40
Число туннелей SSL VPN (по умолчанию/макс.) *6	20/30	20/30	20/60	20/60
Интерфейсы VLAN	8	8	16	16
Число авторизованных пользователей (по умолчанию/ макс.) *7*8	64	64	200	200
Производительность в Speedtest				
Пропускная способность межсетевого экрана SPI (Мбит/сек) *9	320	320	470	470
Управление WLAN				
Число управляемых точек доступа (по умолчанию/макс.) *7	2/18	2/18	2/18	2/18
Рекомендуемое максимальное число точек доступа в 1 группе	10	10	10	10
Сервисы безопасности				
Антивирус (AV) *7	Да	Да	Да	Да
Обнаружение/предотвращение вторжений (IDP) и Патруль приложений *7	Да	Да	Да	Да
Антиспам *7	Да	Да	Да	Да
Контентная фильтрация *7*10	Да	Да	Да	Да
SecuReporter Premium *7	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	-	-	-	-
2-факторная аутентификация	Да	Да	Да	Да
Мастер быстрой настройки	Да	Да	Да	Да
Управление хот-спотами *7	-	-	Да	Да
Поддержка принтеров квитанций *10/ Максимальное число принтеров	-	-	Да (SP350E) / 10	Да (SP350E) / 10

Модель	USG40	USG40W	USG60	USG60W	
Microsoft Azure	Да	Да	Да	Да	
Amazon VPC	Да	Да	Да	Да	
Facebook Wi-Fi	Да	Да	Да	Да	
Device HA Pro	-	-	-	-	
Link Aggregation (LAG)	-	-	-	-	
Требования к питанию					
Источник питания	12 В постоянного тока, 2.0 А максимум	12 В постоянного тока, 2.0 А максимум	12 В постоянного тока, 2.5 А максимум	12 В постоянного тока, 2.5 А максимум	
Максимальное энергопотребление (Ватт)	14	17	19	28	
Тепловыделение (BTU/час)	47.77	58.01	64.83	95.54	
Физические характеристики					
Без упаковки	Размеры (ШхГхВ) (мм)	216 x 143 x 33	216 x 143 x 33	242 x 175 x 36	272 x 187 x 36
	Вес (кг)	0.89	0.91	1.25	1.46
В упаковке	Размеры (ШхГхВ) (мм)	381 x 261 x 79	381 x 261 x 79	394 x 240 x 101	427 x 247 x 73
	Вес (кг)	1.57	1.63	2.25	2.23 (без скоб) 2.42 (со скобами)
Аксессуары в комплекте поставки	<ul style="list-style-type: none"> • Адаптер питания • Кабель DB9- RJ-45 для подключения консоли 	<ul style="list-style-type: none"> • Адаптер питания • Кабель DB9- RJ-45 для подключения консоли • Антенна 	<ul style="list-style-type: none"> • Адаптер питания • Набор для монтажа в стойке 	<ul style="list-style-type: none"> • Адаптер питания • Набор для монтажа в стойке • Антенна 	
Требования к окружающей среде					
Работа	Температура	0°C - +40°C	0°C - +40°C	0°C - +40°C	0°C - +40°C
	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
	Влажность	10% - 90% (без выпадения конденсата)	10% - 90% (без выпадения конденсата)	10% - 90% (без выпадения конденсата)	10% - 90% (без выпадения конденсата)
MTBF (часов)		414329.4	386931.7	815463.9	497644
Сертификаты					
EMC	FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), 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	LVD (EN60950-1), BSMI	

Примечания:

*: 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 AV и IDP измерялась с помощью стандартного теста производительности HTTP (пакеты HTTP по 1460 байтов) с несколькими потоками данных.

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

*6: В том числе Gateway-to-Gateway и Client-to-Gateway.

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

*8: Это число одновременно авторизованных пользователей.

*9: Тесты Speedtest проводились с использованием канала 1 Гбит/с в реальной сети, и на их результаты может повлиять качество канала провайдера.

*10: Функция SafeSearch в CF2.0 доступна с инспекцией SSL и не используется в моделях, предназначенных для малого бизнеса.

*11: Поддерживается с лицензией Hotspot Management.

Спецификация беспроводного интерфейса

Модель	USG40W	USG60W
Соответствие стандартам	802.11 b/g/n	802.11 a/b/g/n
Частота беспроводной связи	2.4 ГГц	Одновременно 2.4 и 5 ГГц
Радиомодуль	1	2
Число SSID	8	16
Макс. мощность передатчика (по всем каналам)	США (FCC) 2.4 ГГц	24.3 дБм 2 антенны
	США (FCC) 5 ГГц	-
	Европа (ETSI) 2.4 ГГц	19.6 дБм (EIRP), 2 антенны
	Европа (ETSI) 5 ГГц	-
Число антенн	2.4 ГГц: 2T2R MIMO (съёмные, SMA-R)	2.4 ГГц: 2T2R MIMO 5 ГГц: 2T2R MIMO (съёмные, SMA-R)
Усиление антенны	3 дБи	3 дБи
Скорость передачи данных	802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 и 54 Мбит/сек 802.11n: до 300 Мбит/сек в MCS15 (40 МГц; GI = 400 нсек)	802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 и 54 Мбит/сек 802.11a: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/сек 802.11n: до 300 Мбит/сек в MCS15 (40 МГц; GI = 400 нсек)
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)	-
Чувствительность приемника	2.4 ГГц	11 Мбит/сек ≤ -87 дБм 54 Мбит/сек ≤ -77 дБм HT20, MCS15 ≤ -71 дБм HT40, MCS15 ≤ -68 дБм
	5 ГГц	-
		США (FCC): 5.150 - 5.250 ГГц; 5.725 - 5.850 ГГц Европа (ETSI): 5.15 - 5.35 ГГц; 5.470 - 5.725 ГГц Тайвань (NCC): 5.25 - 5.35 ГГц; 5.725 - 5.850 ГГц
		* 54 Мбит/сек ≤ -75 дБм * HT20, MCS15 ≤ -71 дБм * HT40, MCS15 ≤ -69 дБм

Функции

Функции программного обеспечения

Межсетевой экран

- Сертифицированный ICASA 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 кастомных портов
- Обнаружение и защита от Техническая спецификация

аномалий протоколов

- Обнаружение и защита от аномалий трафика
- Обнаружение и защита от флуда
- Защита от DoS/DDoS атак
- Поддержка RPS для обеспечения требуемой производительности при нестабильном трафике

Поддержка IPv6

- Двойной стек
- Туннелирование IPv4 (6rd and 6to4 transition tunnel)
- Адреса IPv6
- DNS
- DHCPv6
- Мост

- VLAN
- PPPoE
- Статическая маршрутизация
- Политики маршрутизации
- Контроль сессий
- Межсетевой экран и ADP
- IPSec VPN
- Обнаружение и предотвращение вторжений (IDP)
- Патруль приложений
- Контентная фильтрация
- Антивирус
- Антиспам

IPSec VPN

- Шифрование: AES (256-битное), 3DES и DES
- Аутентификация: MD5, SHA1, SHA2 (512-битная)
- Управление ключами: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Поддержка Perfect forward secrecy (DH groups) 1, 2, 5, 14, 15-18
- IPSec NAT traversal (NAT-T)
- Dead peer detection и relay detection
- Поддержка сертификатов PSK и PKI (X.509)
- Концентратор VPN
- Поддержка Route-based VPN Tunnel Interface (VTI)
- Поддержка мастера быстрой настройки
- Автоматическое повторное соединение VPN
- VPN High Availability (HA): балансировка нагрузки и переключение при отказах
- L2TP over IPSec
- GRE и GRE over IPSec
- NAT over IPSec
- Автоматическая настройка клиентов Zyxel VPN
- Автоматическая настройка клиентов iOS L2TP/IKE/IKEv2 VPN

SSL VPN

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

Обнаружение и предотвращение вторжений (IDP)

- Режим маршрутизации и прозрачный режим (мост)
- Сканирование на основе сигнатур и поведения
- Автоматическое обновление сигнатур
- Настраиваемый профиль защиты
- Поддержка настраиваемых сигнатур

Патруль приложений

- Гранулярный контроль самых важных приложений
- Идентификация и контроль поведения приложений
- Поддержка 15+ категорий приложений
- Управление выделяемой приложениям полосой пропускания
- Поддержка аутентификации пользователей
- Статистика и отчеты в реальном времени
- Поддержка IDP/ADP в социальных сетях, например, для лайков и постов Facebook

Антивирус

- Поддержка сигнатур антивируса
- Идентификация и блокирование более 650 тысяч вирусов
- Поточковый движок антивируса

Техническая спецификация
ZyWALLUSG40/40W/60/60W

- Поддержка протоколов HTTP, FTP, SMTP, POP3 и IMAP4
- Автоматическое обновление сигнатур
- Нет ограничений на размер файла

Антиспам

- Прозрачный перехват почты, которая пересылается по протоколам SMTP и POP3
- Настройка конфигурации портов POP3 и SMTP
- Фильтр репутации IP-адресов отправителей
- Технология Recurrent Pattern Detection (RPD)
- Защита от ранее неизвестных вирусов
- Поддержка X-Header
- Поддержка «черного» и «белого» списка отправителей
- Поддержка проверки DNSBL
- Поддержка тегов спама
- Статистические отчеты

Контентная фильтрация

- Фильтр социальных сетей
- Фильтр опасных Web-сайтов
- Блокирование по URL и ключевым словам
- Поддержка «черного» и «белого» списка отправителей
- Блокирование апплетов java, cookies и ActiveX
- Облачная постоянно обновляемая база данных URL
- Лицензия без ограничений на число пользователей
- Настраиваемые предупреждения и перенаправление URL
- Фильтр доменов HTTPs
- Блокирование IP-адресов по геопризнакам
- Мониторинг трафика в соответствии с местным законодательством

Унифицированная политика

безопасности

- Унифицированный интерфейс управления политикой безопасности
- Поддерживаемые функции UTM: антивирус, антиспам, IDP, контентная фильтрация, патруль приложений, межсетевой экран (ACL)
- 3-уровневое конфигурирование: на базе объектов, на базе профилей и на базе политик
- Критерии политики: зона, IP-адреса отправителя и получателя, пользователь, время
- Заранее определенные профили UTM для разных групп пользователей

Управление беспроводной сетью

- Поддержка контроллера точек доступа (APC) v3.40
- Изоляция на уровне L2

- 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 для стабильного и надежного покрытия
- Аутентификация IEEE 802.1x
- Настраиваемый web-портал авторизации
- Авторизация RADIUS
- Поддержка Wi-Fi Multimedia (WMM)
- Поддержка протокола обнаружения CAPWAP
- Мульти-SSID с VLAN
- Поддержка ZyMesh
- Поддержка совместимых точек доступа

Управление хот-спотами*

- Интегрированные генератор учетных записей, Web-портал аутентификации и биллинговая система
- Поддержка внешних серверов RADIUS
- Управление полосой пропускания, выделяемой отдельным учетным записям
- Вход с подтверждением пользовательского соглашения
- Создание учетной записи пользователя и выставление счета одним движением при помощи принтера квитанций SP350E
- Встроенная биллинговая система
 - Режим учета оставшегося времени (Time-to-Finish)
 - Режим учета суммарного использованного времени (Accumulation accounting)
- Поддержка онлайн-платежей PayPal
- Инструменты для маркетинга
 - Ссылка на рекламу
 - Walled garden
 - Страница портала

• Пополнение счета
* Поддерживают только USG60/60W с микропрограммой ZLD версии 4.35 или более поздней

Широкополосный доступ по сотовой сети

- Резервный канал WAN с использованием USB-модема 3G или 4G*
 - Автоматическое переключение на основной канал WAN после восстановления его работоспособности
- * Поддерживаемые USB-модемы 3G и 4G указаны в соответствующем списке продукта на web-сайте Zyxel.

Сетевое 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)
- 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
- GRE
- BGP

Аутентификация

- Локальная база данных пользователей
- Интеграция с Microsoft Windows Active Directory
- Внешняя база данных пользователей LDAP/RADIUS
- Аутентификация XAUTH, IKEv2 с EAP VPN
- Аутентификация через Web

- Принудительная аутентификация пользователей (прозрачная аутентификация)
- Привязка адресов IP-MAC
- Поддержка SSO (Single Sign-On)

Управление системой

- Ролевое администрирование
- Несколько учетных записей администратора
- Поддержка Cloud Helper
- Многоязычный web-интерфейс (HTTPS и HTTP)
- Интерфейс командной строки (консоль, web-консоль, SSH и telnet)
- SNMP v1, v2c, v3
- «Откат» к предыдущей конфигурации системы
- Обновление микропрограммы с использованием FTP, FTP-TLS и Web
- 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
- Облачный сервис аналитики и подготовки отчетов SecuReporter

Zyxel One Network

- Утилита ZON
 - Конфигурирование IP -адресов
 - Доступ к Web-интерфейсу
 - Обновление микропрограммы
 - Конфигурирование паролей
- Smart Connect
 - Обновление системного имени и расположения
 - Обнаружение соседних устройств
 - Доступ к удаленному управлению соседними устройствами Zyxel одним щелчком мыши

Пакеты лицензий

Безопасность

Продукт	Антивирус	Патруль приложений и IDP	Контентная фильтрация	Антиспам	SecuReporter Premium
USG40/40W	1 год/2 года	1 год/2 года	1 год/2 года	1 год/2 года	1 год/2 года
USG60/60W	1 год/2 года	1 год/2 года	1 год/2 года	1 год/2 года	1 год/2 года

1. Вместе с Zyxel USG можно приобрести стандартную лицензию на 12 месяцев (антивирус, антиспам, контентная фильтрация, IDP и SecuReporter) с дополнительным ознакомительным использованием в течение 1 месяца.

2. С помощью портала myZyxeI можно легко активировать лицензии, продлевать и управлять ими.

3. Состав пакетов лицензий может отличаться в зависимости от вашего региона. Для уточнения обратитесь в местное торговое представительство ZyxeI.

Решения VPN и Wi-Fi промышленного класса

Продукт	Туннели SSL VPN	Клиент SSL VPN *	Клиент IPSec VPN
USG40/40W	Дополнительно 5/10 туннелей	Для 1/5/10 клиентов	Для 1/5/10/50 клиентов
USG60/60W	Дополнительно 5/10 туннелей	Для 1/5/10 клиентов	Для 1/5/10/50 клиентов

*: Поддерживаемые операционные системы: MAC OS 10.7 и более поздней версии

Продукт	Управление хот-спотами	Управляемые точки доступа
USG40/40W	-	Дополнительно 2/4/8 точек доступа
USG60/60W*	1 год/бессрочно	Дополнительно 2/4/8 точек доступа

*: : С микропрограммой ZLD версии 4.35 или более поздней

Список совместимых точек доступа

Продукт	Точки доступа серии Unified	Точки доступа серии Unified Pro
Модели	<ul style="list-style-type: none"> • NWA5121-NI • NWA5121-N • NWA5123-NI • NWA5123-AC 	<ul style="list-style-type: none"> • NWA5123-AC HD • NWA5301-NJ • WAC5302D-S • Совместимые точки доступа*
		<ul style="list-style-type: none"> • WAC6103D-I • WAC6303D-S • WAC6502D-E • WAC6502D-S
		<ul style="list-style-type: none"> • 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, шлюзы коммерческого класса 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.

Аксессуары

Программное обеспечение SecuExtender

Клиентское ПО	Описание	Поддерживаемые операционные системы
IPSec VPN Client*	Программный клиент IPSec VPN для ZyWALL и USG с поддержкой Easy VPN для автоматической настройки удаленного доступа	<ul style="list-style-type: none"> • Windows XP (32-bit) • Windows Server 2003 (32-bit) • Windows Server 2008 (32/64-bit) • Windows Vista (32/64-bit) • Windows 7 (32/64-bit) • Windows 8 (32/64-bit) • Windows 10 (32/64-bit)
SSL VPN Client*	Защищенное соединение VPN между PC/MAC и ZyWALL	<ul style="list-style-type: none"> • Windows 7 (32/64-bit) • Windows 8/8.1 (32/64-bit) • Windows 10 (32/64-bit) • MAC OS 10.7 или новее

*: 30-дневную ознакомительную версию программных клиентов IPSec VPN и SSL VPN для MAC OS можно загрузить с официального web-сайта Zyxel. Для продолжения использования приложения нужно приобрести лицензию у местного торгового представителя Zyxel.

ZYXEL

Your Networking Ally

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



Copyright © 2019 Zyxel Communications Corp. Все права защищены. Zyxel и логотип Zyxel являются зарегистрированными торговыми марками Zyxel Communications Corp. Все другие упоминаемые бренды, названия продуктов и торговые марки являются собственностью соответствующих владельцев. Все спецификации могут быть изменены без письменного уведомления.

04/10/19