ZyXEL

Межсетевые экраны ZyWALL и центры безопасности USG

для малого и среднего бизнеса

Решения сетевой безопасности от ZyXEL

Унифицированные центры безопасности USG и межсетевые экраны ZyWALL нового поколения — это компактные высокоинтегрированные устройства, предназначенные для решения широкого спектра задач по построению IT-инфраструктуры предприятий малого и среднего бизнеса, в числе которых бесперебойное подключение к Интернету, создание безопасных каналов связи с удаленными подразделениями и сотрудниками, а также всесторонняя защита IT-инфраструктуры от угроз из Интернета и оптимизация ее работы.

Высокая производительность

Сочетая в себе новую аппаратную платформу, основанную на многоядерных процессорах Cavium Octeon, и проверенную временем операционную систему ZLD, устройства ZyWALL и USG дают малому и среднему бизнесу впечатляющий набор функций и одни из лучших показателей производительности в отрасли, что подтверждают результаты тестов независимых экспертов.

Множественные интерфейсы WAN

Множественные гигабитные интерфейсы WAN и порты USB для подключения модемов 3G/4G позволяют реализовать резервирование и балансировку нагрузки каналов Интернета и туннелей VPN, что обеспечивает надежную связь с удаленными подразделениями и бесперебойный доступ к сервисам Интернета, необходимым для ведения бизнеса.

Виртуальные частные сети

Отвечая тенденциям глобализации и мобильности бизнес-процессов, USG и ZyWALL имеют богатый арсенал функций VPN для создания высокоскоростных защищенных каналов связи с удаленными подразделениями, партнерами и выездными сотрудниками. Благодаря этому предприятия могут объединять свои многочисленные географически разнесенные подразделения в единую информационную инфраструктуру, а также создавать мобильные рабочие места на базе смартфонов, планшетов и ноутбуков для выездных сотрудников, позволяя им мгновенно решать многие рабочие вопросы вне офиса, что значительно ускоряет бизнес-процессы.

Всесторонняя защита от угроз из Интернета

Устройства ZyWALL и USG предоставляют целый ряд сервисов сетевой безопасности, таких как встроенный потоковый антивирус (AV), система обнаружения и предотвращения вторжений (IDP), патруль приложений (AP), контентная фильтрация (CF) и фильтрация спама (AS). Благодаря этим сервисам ZyWALL и USG способны защитить малый и средний бизнес от проникновения в корпоративную сеть вредоносных программ, атак хакеров, ограничить доступ сотрудников к нежелательным ресурсам Интернета и остановить лавину нежелательных сообщений, рассылаемых по электронной почте.

Управление полосой пропускания

Встроенный инструментарий управления полосой пропускания BWM позволяет обеспечить наилучшее качество обслуживания для трафика бизнес-приложений, чувствительных к задержкам и потерям передаваемых данных, например таким, как IP-телефония и видеоконференцсвязь. Интеграция BWM с сервисом Application Patrol позволит взять под контроль в т.ч. клиенты пиринговых сетей, программы мгновенного обмена сообщениями и т.п.

Средства для интеграции в существующую IT-инфраструктуру

Встроенная поддержка LDAP/MS AD/RADIUS помогает структурировать политики безопасности на основе уже существующей методики организации сети.

Поддержка прозрачной аутентификации пользователей MS Active Directory с технологией Single Sign-ON значительно упрощает интеграцию устройств ZyWALL и USG в уже существующую IT-инфраструктуру на базе решений от Microsoft.

Встроенный контроллер беспроводных сетей

Встроенный контроллер беспроводных сетей позволяет развертывать и централизованно администрировать беспроводные сегменты сети на базе профессиональных точек доступа Wi-Fi серии NWA/WAC от компании ZyXEL. Высокое качество обслуживания беспроводных клиентов обеспечивают технологии, использованные ранее только на профессиональных контроллерах ZyXEL серии NXC.

Поддержка IPv6

Поддержка протокола IPv6, включая двойной стек IPv4/IPv6, IPv6 IPSec и IPv6 UTM, позволит компаниям избежать затрат на новое IPv6-совместимое оборудование в процессе миграции корпоративных сетей к инфраструктуре IPv6, сохраняя высокий уровень сетевой безопасности и оправдывая инвестиции в ZyWALL и USG.

Средства мониторинга и управления

Межсетевые экраны ZyWALL и центры безопасности USG оснащены интуитивно понятным пользовательским веб-интерфейсом с перекрестной системой навигации, встроенным справочником, мастером настройки основных функций и графическим мониторингом состояния. Объектно-ориентированная модель управления максимально упрощает настройку даже в сложных сетях. Встроенные средства мониторинга и диагностики сети позволяют получать детальную информацию по сетевому трафику, сессиям, работе беспроводной сети, активности пользователей, обнаруженным угрозам и т.п. Для настройки сети и сбора статистики о ее работе доступны утилиты ZyXEL One Network Utility и Vantage Report. Все эти функции дают IT-персоналу широкие возможности для развертывания и администрирования сетевой инфраструктуры предприятия.

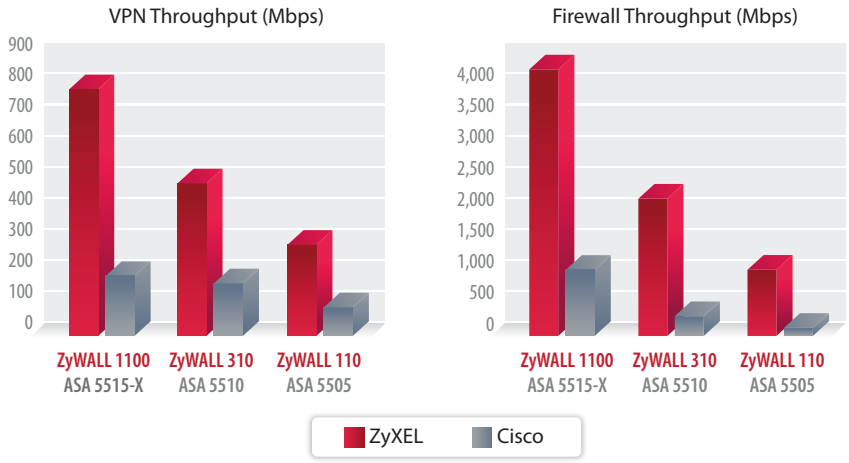
При всех своих широких функциональных возможностях межсетевые экраны ZyWALL и центры безопасности USG являются компактными, простыми и надежными в эксплуатации устройствами с привлекательным соотношением цены и качества, внедрение и эксплуатация которых не требуют существенных финансовых и трудовых затрат.

Компания ZyXEL непрерывно работает над совершенствованием устройств ZyWALL и USG, оптимизирует их работу и добавляет новые необходимые пользователям функции. Результатом этой работы является регулярный выпуск новых микропрограмм, которые бесплатно доступны всем пользователям устройств ZyWALL и USG.

Функциональные особенности ZyWALL и USG

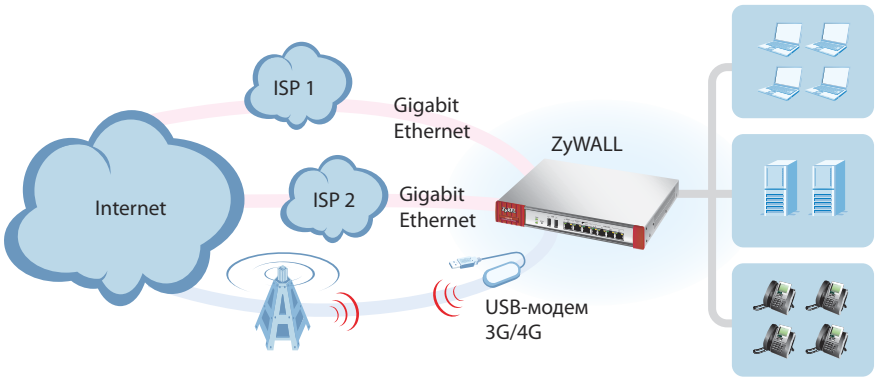
Высокая производительность

Межсетевые экраны ZyWALL и центры безопасности USG нового поколения оснащены высокопроизводительными многоядерными процессорами Cavium Octeon. По пропускной способности межсетевого экрана (до 7 Гбит/с) и VPN (до 900 Мбит/с) эти устройства не только многократно опережают модели ZyWALL USG прошлого поколения, но и являются одними из самых производительных по сравнению с конкурирующими продуктами других производителей, представленными на рынке. Устройства ZyWALL и USG, разработанные на основе новых, передовых технологий с бескомпромиссной производительностью, гарантируют высокую эффективность коммуникаций для успешного ведения бизнеса.



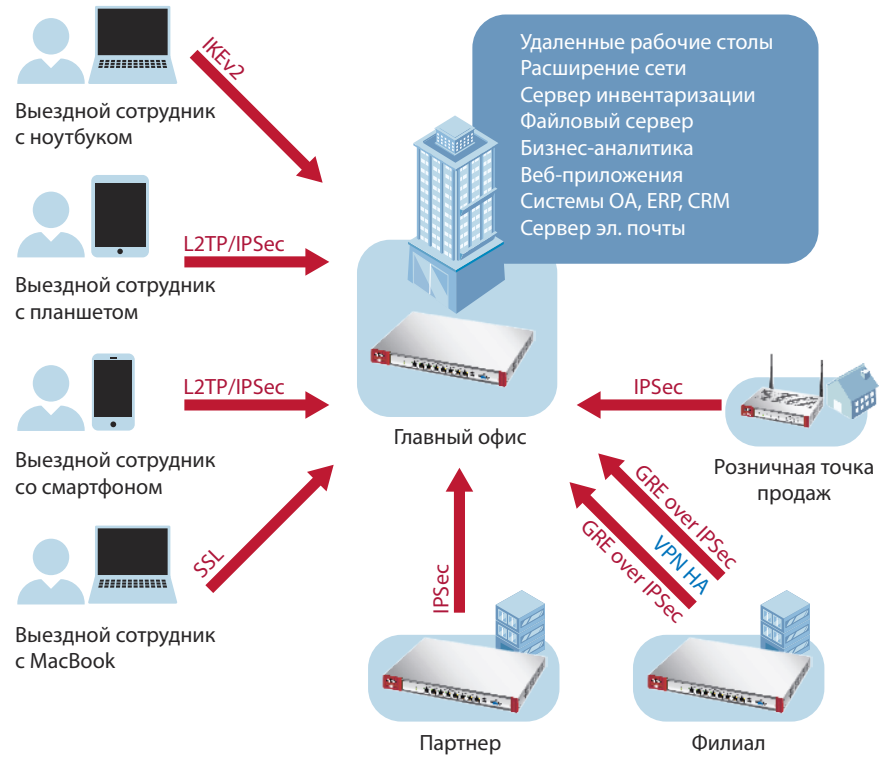
Бесперебойный доступ в Интернет

При выполнении повседневных операций бизнеса недоступность каналов подключения к Интернету негативно отражается на работе организации. Устройства ZyWALL и USG позволяют решить эту проблему. Благодаря множественным портам WAN они могут использовать одновременно несколько каналов Интернета от разных интернет-провайдеров. Балансировка нагрузки каналов, автоматическое переключение на резервный канал в случае отказа основных, возврат на основной канал при возобновлении функционирования и использование 3G/4G-модема в качестве основного или резервного канала – все эти функции могут обеспечить бесперебойный доступ в Интернет 24 часа в сутки.



Технологии VPN

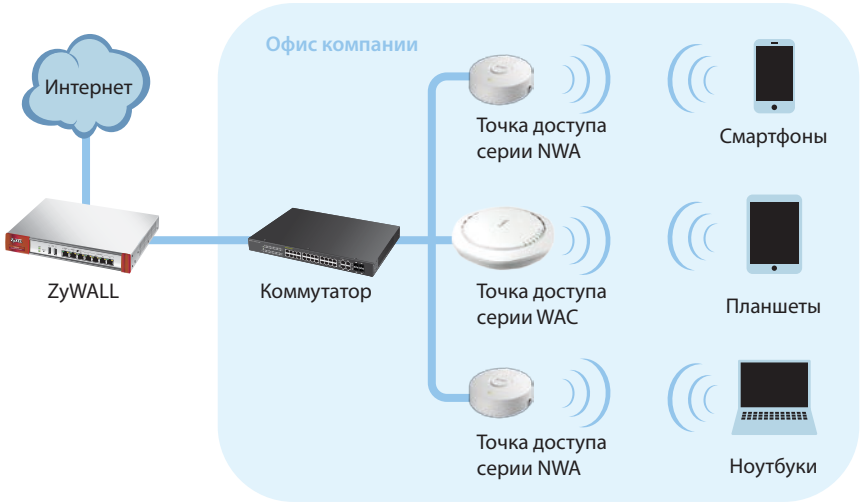
Благодаря поддержке IPSec VPN компании могут создавать защищенные каналы для связи удаленных подразделений с головным офисом. Бесперебойная работа туннелей VPN достигается путем резервирования VPN через несколько каналов Интернета от разных провайдеров, подключаемых к множественным интерфейсам WAN. Кроме того, имеется возможность объединять VPN-туннели, созданные через разные каналы Интернета в транк с балансировкой нагрузки, тем самым увеличивая суммарную пропускную способность соединения между удаленным подразделением и главным офисом. Сотрудники, находящиеся в пути или работающие дома, могут воспользоваться защищенным удаленным доступом к ресурсам сети компании с использованием технологий SSL, IKEv2 или L2TP/IPSec, которые штатно поддерживаются операционными системами MS Windows, iPhone iOS, Mac OS X и Android. Благодаря этому каждый сотрудник компании, находящийся вне офиса, может в любой момент подключиться к корпоративной сети со своего смартфона или планшета и решить многие рабочие вопросы вне офиса, что значительно ускоряет бизнес-процессы.



Функциональные особенности ZyWALL и USG

Контроллер беспроводных сетей

Контроллер беспроводных сетей, интегрированный в ZyWALL и USG нового поколения, позволяет с легкостью развертывать, масштабировать и централизованно администрировать беспроводную сеть компании с использованием управляемых точек беспроводного доступа ZyXEL серии NWA/WAC с поддержкой диапазонов 2,4 ГГц и 5 ГГц. Высокое качество обслуживания беспроводных клиентов обеспечивают технологии, в числе которых балансировка нагрузки точек по количеству клиентов и величине трафика, управление распределением полосы пропускания между клиентами, поддержание заданного уровня сигнала при роуминге клиента между точками в зоне покрытия и автоматический выбор наименее зашумленных радиоканалов для передачи данных.



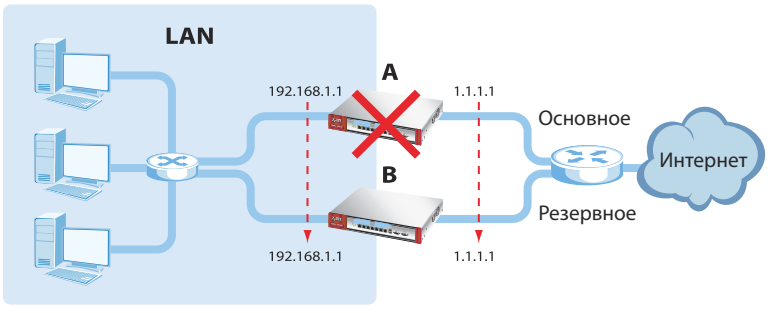
Интеграция с MS Active Directory

Технология Single Sign-On (SSO) предназначена для интеграции устройств ZyWALL и USG нового поколения в IT–инфраструктуру на базе Microsoft Active Directory. С ее помощью осуществляется прозрачная аутентификация пользователей MSAD на устройствах. Бесплатное приложение SSO Agent, устанавливаемое на сервер Windows 2008/2012 для связи с контроллером домена, отправляет уведомления на устройство при каждом успешном входе/выходе пользователя в домен/из домена. Получая уведомление о входе в домен, устройство ZyWALL/USG авторизует пользователя с применением соответствующих политик безопасности, сконфигурированных на устройстве IT-персоналом. Благодаря технологии SSO пользователям MSAD не требуется выполнять дополнительную аутентификацию на ZyWALL/USG. Будучи авторизованными контроллером домена, они будут автоматически авторизованы и устройством ZyWALL/USG.

Резервирование устройства

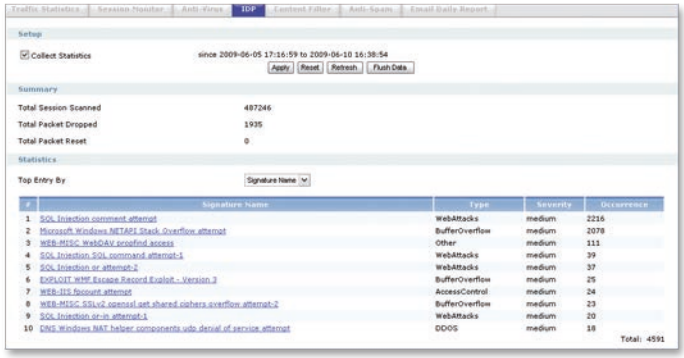
Резервирование устройства (Device HA) гарантирует круглосуточную бесперебойную работу корпоративной сети, построенной на базе устройств ZyWALL и USG. Это достигается одновременным использованием двух одинаковых устройств: основного и резервного. В случае временного сбоя или выхода из строя основного устройства все его функции автоматически берет на себя резервное устройство.

Резервирование на уровне устройства: основное устройство выходит из строя, вместо него подключается резервное



Мониторинг и диагностика сети

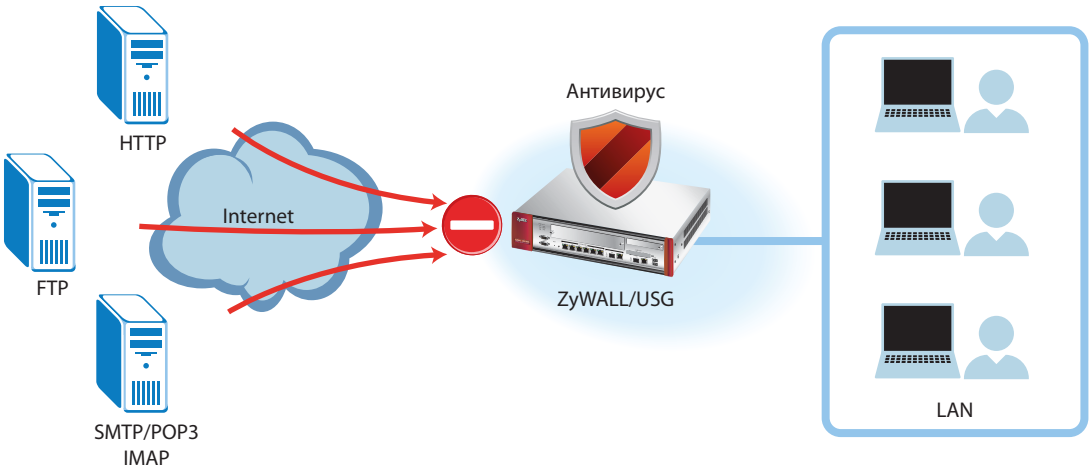
Межсетевые экраны ZyWALL и центры безопасности USG имеют встроенные средства мониторинга для получения детальной информации по сетевому трафику, сессиям, туннелям VPN, активности пользователей, функционированию беспроводной сети, обнаруженным угрозам и т.п. Для диагностики сети можно воспользоваться встроенными утилитами PING IPv4/IPv6 и TRACEROUTE IPv4/IPv6, возможностью захвата трафика на любых интерфейсах и наглядным графическим представлением правил маршрутизации, действующих на устройстве.



Технологии сетевой безопасности ZyWALL и USG

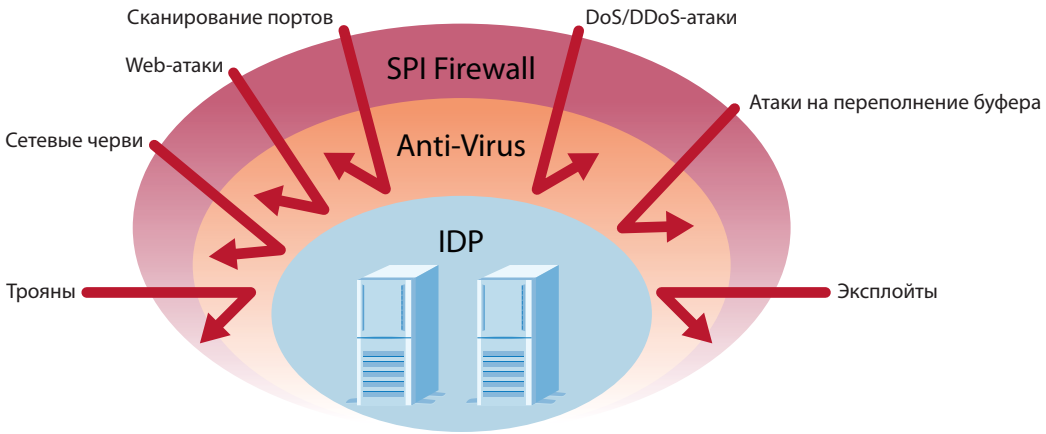
Антивирус (Anti-Virus, AV)

Проникновение вирусов, троянов, сетевых червей и других вредоносных программ из Интернета в корпоративную сеть может вызвать нарушение работы сети и приостановить нормальное течение бизнеса. Помимо нанесения финансового ущерба, это может вызвать утечку важной конфиденциальной информации. Являясь первым рубежом антивирусной обороны на границе сети, встроенный в ZyWALL и USG потоковый антивирус препятствует проникновению вредоносных программ в корпоративную сеть. Сканированию подвергаются файлы любого размера, передаваемые по протоколам HTTP, FTP, SMTP, POP3 и IMAP4 через устройство. Поддерживается сканирование архивов ZIP, GZIP, PKZIP и RAR. Эффективную защиту от вирусов и высокую производительность при сканировании обеспечивает интеграция технологии SafeStreamII Лаборатории Касперского с аппаратными возможностями многоядерных процессоров Cavium Octeon. Ежедневно обновляемая база вирусных сигнатур позволяет обнаружить более 600 000 вредоносных программ.



Предотвращение вторжений (Intrusion Detection&Prevention, IDP)

Корпоративные сети предприятий регулярно подвергаются атакам хакеров, направленным на получение контроля над компьютерными системами и сбор ценной конфиденциальной информации и интеллектуальной собственности предприятия. Обычные межсетевые экраны и антивирусные средства не способны противостоять все более изощренным сетевым атакам уровня приложений. Система обнаружения и предотвращения вторжений, встроенная в устройства ZyWALL и USG, обнаруживает и блокирует атаки DoS и DDoS, активность сетевых червей, троянов, бэкдоров и эксплойтов, использующих уязвимости операционных систем и прикладных программ, а также противодействует разведывательным действиям и атакам, использующим сканирование и флуд. Обнаружение вредоносных проявлений достигается путем анализа проходящего через устройство сетевого трафика на 4 — 7 уровнях OSI с использованием автоматически обновляемой базы из 3000+ сигнатур, поставляемых компанией Trend MICRO.



Технологии сетевой безопасности ZyWALL и USG

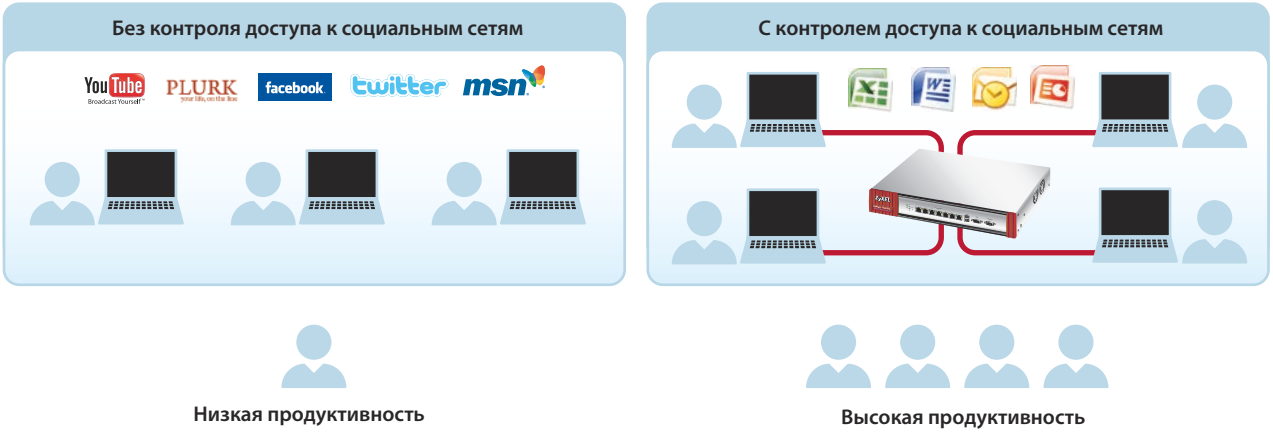
Патруль приложений (Application Patrol, AP)

Нежелательные, не имеющие отношения к рабочему процессу сетевые приложения пользователей, такие как программные клиенты пиринговых и социальных сетей, потокового вещания, обмена мгновенными сообщениями и т.п., могут привести к бесполезной трате пропускной способности корпоративной сети и каналов Интернета и поставить под угрозу безопасность компании. Встроенный сервис Патруль приложений от компании TREND Micro позволяет обнаруживать и ограничивать/блокировать трафик нежелательных приложений, а также обеспечивает гарантированную полосу пропускания для полезного трафика, например IP-телефонии. Контроль сетевых пакетов вплоть до 7 уровня OSI с использованием регулярно обновляемой базы сигнатур гарантирует обнаружение более 3000 популярных приложений из следующих категорий:

- Пиринговые сети
- Файлообменные ресурсы и клиенты
- Потоковая передача данных
- Электронная почта
- IP-телефония
- Базы данных
- Игры
- Управление сетью
- Удаленный терминальный доступ
- Прокси-серверы и VPN
- Фондовая биржа
- Обновления безопасности
- Веб-пейджеры
- Бизнес-приложения
- Мобильные устройства
- Защищенные протоколы веб-пейджеров
- Социальные сети

Контентная фильтрация (Content Filtering, CF)

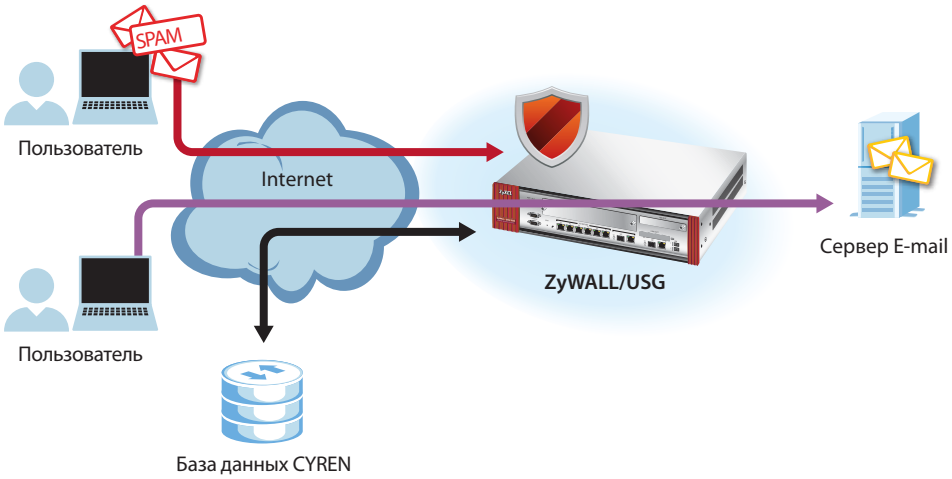
Отсутствие гибкого управления доступом к ресурсам Интернета может негативно сказаться на производительности труда сотрудников и поставить под угрозу безопасность компании. Благодаря встроенному сервису контентной фильтрации устройства ZyWALL и USG могут ограничить доступ сотрудников к интернет-сайтам, не имеющим отношения к рабочим вопросам, а также исключить доступ к потенциально опасным сайтам. Встроенный в ZyWALL и USG сервис контентной фильтрации от компании CYREN в режиме реального времени определяет категории запрашиваемых сайтов, различая 64 категории – от "бизнеса и экономики" до "игр" и "спорта". Это позволяет запретить определенным сотрудникам доступ к определенным категориям сайтов. Встроенные средства мониторинга формируют детальные отчеты о посещаемых сотрудниками сайтах.



Технологии сетевой безопасности ZyWALL и USG

Фильтрация спама (Anti-Spam, AS)

Сервис Антиспам, реализованный в устройствах ZyWALL и USG, способен оградить сотрудников предприятия от лавины бесполезных и потенциально опасных сообщений e-mail, рассылаемых с целью распространения рекламы, вредоносных программ, хищения конфиденциальной информации и т.п. Основанная на облачных технологиях компании CYREN – ведущего в отрасли производителя решений для защиты корпоративных ресурсов в Интернете, – система Anti-Spam позволяет обнаруживать во входящем трафике SMTP и POP3 до 99% спама, подвергая антивирусной проверке файлы во вложениях и эффективно отличая спам от полезных почтовых рассылок, ожидаемых пользователями. Фильтрация спама происходит на границе сети, что значительно снижает нагрузку на почтовый сервер предприятия. С технологиями CYREN эффективное обнаружение спама становится возможным уже через считаные минуты после инициализации спамерских рассылок и не зависит от формата, языка и кодировки сообщений.

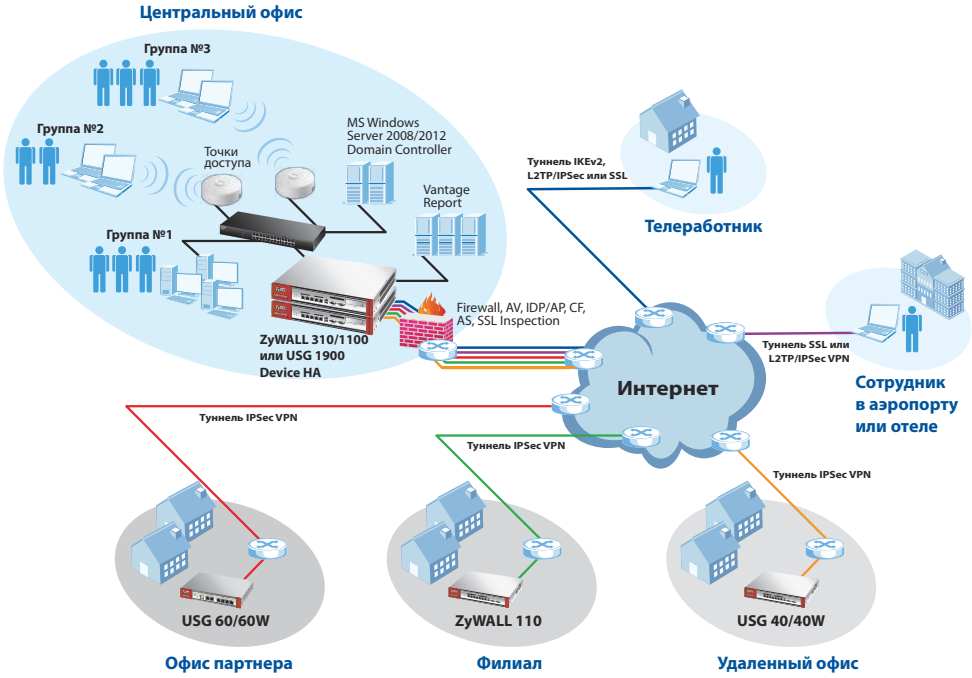


Инспектирование SSL (SSL Inspection)

Многие веб-ресурсы (например, Facebook, Dropbox, Gmail и ВКонтакте), сетевые приложения и вредоносные программы используют шифрование SSL при обмене данными через Интернет. Шифрованный трафик невозможно инспектировать, что создает брешь в системе сетевой безопасности. Технология инспектирования SSL, реализованная в устройствах ZyWALL и USG, способна решить эту проблему. Проходящий через устройство трафик SSL расшифровывается для инспектирования сервисами AV, IDP, AP и CF, затем шифруется снова и передается адресату. В целях соблюдения конфиденциальности сотрудников доверенные интернет-ресурсы, например интернет-банки, медицинские учреждения, электронные сервисы правительства и т.п., могут быть занесены в отдельный список, чтобы исключить дешифрование и инспектирование трафика пользователей этих ресурсов.

Сценарии применения ZyWALL и USG

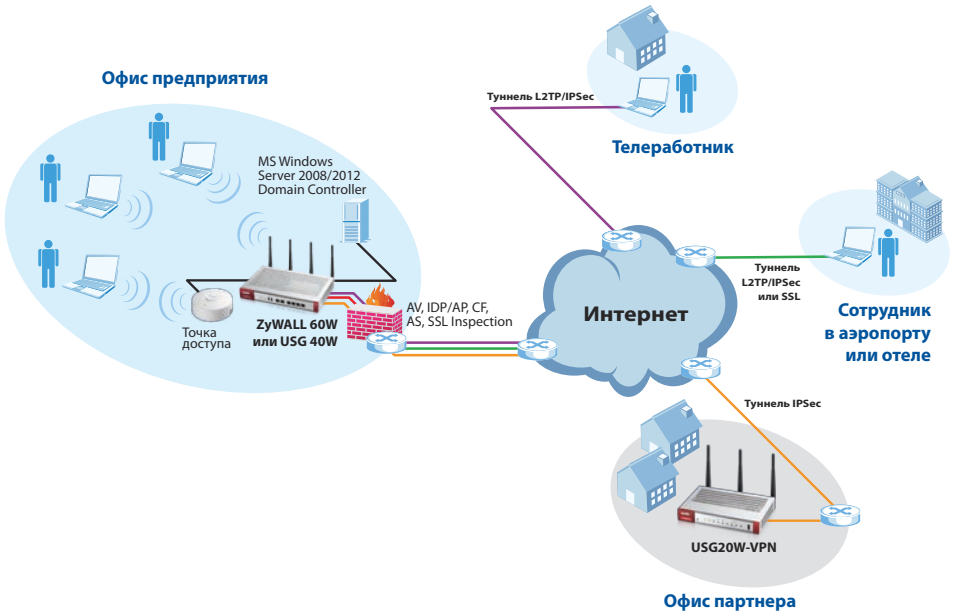
Сценарий применения для среднего бизнеса (до 1000 сотрудников)



В центральном офисе предприятия используются два устройства одной из старших моделей ZyWALL или USG в режиме Device HA, что гарантирует бесперебойную работу сети предприятия 24 часа в сутки. Беспроводная сеть построена на базе встроенного контроллера WLAN, управляющего точками доступа Wi-Fi серии NWA/WAC. Подключение к Интернету резервировано путем одновременного использования нескольких каналов Интернета от разных провайдеров, подключенных к внешним интерфейсам устройства. Для защиты IT-инфраструктуры компании от угроз из Интернета используются встроенные сервисы безопасности AV, IDP, AP, CF и AS, которые инспектируют весь интернет-трафик. Защищенные каналы связи с филиалами и партнерами реализованы с помощью младших моделей ZyWALL и USG, соединенных туннелями IPSec VPN с устройством в главном офисе. Выездные сотрудники удаленно подключаются к главному офису со своих смартфонов, планшетов и ноутбуков, используя технологии IKEv2, L2TP/IPSec и SSL.

Для интеграции ZyWALL/USG с доменом MSAD используется технология SSO. Это позволяет аутентифицировать на устройстве локальных и удаленных пользователей AD и создавать индивидуальные политики доступа к бизнес-приложениям и ресурсам Интернета. Для централизованного сбора, хранения и обработки статистических данных о работе сети используется программа Vantage Report.

Сценарий применения для малого бизнеса (менее 10 сотрудников)



В офисе малого предприятия используется центр безопасности USG 40/40W или USG 60/60W. Беспроводная сеть предприятия построена на базе встроенной точки доступа Wi-Fi. При необходимости беспроводную сеть можно расширить, подключая внешние точки доступа Wi-Fi серии NWA/WAC. Встроенный контроллер WLAN управляет как встроенной точкой, так и внешними точками, обеспечивая бесшовный роуминг и высокое качество обслуживания беспроводных клиентов. Подключение офиса к Интернету резервировано путем одновременного использования нескольких каналов Интернета от разных провайдеров. Для беспроводного подключения к Интернету можно использовать USB-модем 3G/4G. Интеграция USG с доменом MSAD позволяет аутентифицировать на устройстве локальных и удаленных пользователей AD и создавать индивидуальные политики доступа к бизнес-приложениям на сервере предприятия и ресурсам Интернета. Встроенные сервисы безопасности AV, IDP, AP, CF и AS защищают IT-инфраструктуру компании от вирусов, сетевых атак и спама, а также ограничивают доступ сотрудников к ресурсам Интернета, не имеющим отношения к рабочему процессу. Защищенные каналы связи с партнерами реализованы с использованием технологии IPSec VPN. Выездные сотрудники удаленно подключаются к главному офису со своих смартфонов, планшетов и ноутбуков, используя технологии IKEv2, L2TP/IPSec и SSL, которые штатно поддерживаются операционными системами мобильных устройств.

Сравнительная таблица характеристик ZyWALL и USG




Модель	USG20/20W-VPN	USG 40/40W	USG 60/60W	ZyWALL 110
Система				
Пропускная способность SPI Firewall, Мбит/с	350	400	1000	1600
Пропускная способность VPN (AES), Мбит/с	90	100	180	400
Пропускная способность UTM (FW+AV+IDP), Мбит/с	—	50	90	250
Макс. количество сессий NAT (общее/в секунду)	20 000	20 000/3 000	40 000/3 000	60 000/3 500
Макс. число одновременных туннелей IPSec VPN	10	20	40	100
Макс. число одновременных туннелей SSL VPN (базовая комплектация/с лицензией)	5/15	5/15	5/20	25/150
Физические порты GbE	2 порта WAN (1GE+1SFP) 4 порта LAN/DMZ	1 порт WAN 1 порт WAN/LAN/DMZ 3 порта LAN/DMZ	2 порта WAN 4 порта LAN/DMZ	1 порт WAN 1 порт WAN/LAN/DMZ 4 порта LAN/DMZ
Слоты SFP	1	—	—	—
Порты USB	1	1	2	2
Виртуальные интерфейсы VLAN 802.1q	8	8	16	16
Сеть				
Поддержка IPv4/IPv6	Да	Да	Да	Да
Поддержка режимов Routing и Transparent Bridge	Да	Да	Да	Да
Поддержка IGMP v1/v2 (IGMP proxy)	Да	Да	Да	Да
Управление пропускной способностью (BWM)	Да	Да	Да	Да
Поддержка USB-модемов 3G/4G	Да	Да	Да	Да
Встроенный контроллер WLAN				
Поддерживаемые точки доступа Wi-Fi	—	NWA3160-N, NWA3560-N, NWA3550-N, NWA5160N, NWA5560-N, NWA5550-N, NWA5121-NI, NWA5121-N, NWA5123-NI, NWA5123-AC, NWA5301-NJ WAC6503D-S, WAC6502D-S, WAC6502D-E, WAC6553D-E, WAC6103D-I		
Макс. кол-во управляемых точек доступа (базовая комплектация/с лицензией)	—	2/18	2/18	2/34
Поддержка радиоинтерфейсов 2,4 ГГц и 5 ГГц	—	Да	Да	Да
Встроенный интерфейс WLAN				
Поддерживаемые стандарты сетей Wi-Fi	802.11a/b/g/n/ac	802.11b/g/n	802.11a/b/g/n	—
Радиоинтерфейс 2,4 ГГц	Да	Да	Да	—
Радиоинтерфейс 5 ГГц	Да	—	Да	—
Безопасность				
Межсетевой экран (SPI Firewall)	Да	Да	Да	Да
Поддержка IPSec VPN	Да	Да	Да	Да
Поддержка SSL VPN	Да	Да	Да	Да
Поддержка L2TP/IPSec VPN	Да	Да	Да	Да
Антивирус (AV)	—	Да	Да	Да
Предотвращение вторжений (IDP)	—	Да	Да	Да
Патруль приложений (AP)	—	Да	Да	Да
Фильтрация веб-контента (CF)	Да	Да	Да	Да
Фильтрация спама (AS)	Да	Да	Да	Да
Инспектирование SSL	—	—	—	Да
Резервирование				
Резервирование WAN	Да	Да	Да	Да
Резервирование IPSec VPN	Да	Да	Да	Да
Резервирование устройства (Device HA)	—	—	—	Да
Аутентификация пользователей				
Локальная база данных	Да	Да	Да	Да
RADIUS	Да	Да	Да	Да
Прозрачная аутентификация пользователей MSAD (Single Sign-On)	Да	Да	Да	Да
Администрирование				
Графический веб-интерфейс (HTTP и HTTPS)	Да	Да	Да	Да
Командная строка (SSH, Telnet)	Да	Да	Да	Да
ZyXEL One Network (ZON)	Да	Да	Да	Да
Vantage Report	—	Да	Да	Да
Физические характеристики				
Габариты, мм (Ш x Г x В)	216 x 143 x 33	216 x 143 x 33	242 x 175 x 36 (60) 272 x 171 x 36 (60W)	300 x 178 x 44
Масса, кг	0,90(20) / 1,00(20W)	0,89 (40) / 0,91 (40W)	1,25 (60) / 1,46 (60W)	2

Сравнительная таблица характеристик ZyWALL и USG




Модель	ZyWALL 310	ZyWALL 1100	USG 1900	USG 2000
Система				
Пропускная способность SPI Firewall, Мбит/с	5000	6000	7000	2000
Пропускная способность VPN (AES), Мбит/с	650	800	900	600
Пропускная способность UTM (FW+AV+IDP), Мбит/с	400	500	600	400
Макс. количество сессий NAT (общее/в секунду)	100 000/12 000	500 000/12 000	500 000/12 000	1 000 000/20 000
Макс. число одновременных туннелей IPSec VPN	300	1 000	2 000	2 000
Макс. число одновременных туннелей SSL VPN (базовая комплектация/с лицензией)	50/150	250/500	750	750
Физические порты GbE	8 портов WAN/LAN/DMZ	8 портов WAN/LAN/DMZ	8 портов WAN/LAN/DMZ	8 портов WAN/LAN/DMZ
Слоты SFP	—	—	—	2
Порты USB	2	2	2	2
Виртуальные интерфейсы VLAN 802.1q	50	128	128	512
Сеть				
Поддержка IPv4/IPv6	Да	Да	Да	Да
Поддержка режимов Routing и Transparent Bridge	Да	Да	Да	Да
Поддержка IGMP v1/v2 (IGMP proxy)	Да	Да	Да	—
Управление пропускной способностью (BWM)	Да	Да	Да	Да
Поддержка USB-модемов 3G/4G	Да	Да	Да	3G/-
Встроенный контроллер WLAN				
Поддерживаемые точки доступа Wi-Fi	NWA3160-N, NWA3560-N, NWA3550-N, NWA5160N, NWA5560-N, NWA5550-N, NWA5121-NI, NWA5121-N, NWA5123-NI, NWA5123-AC, NWA5301-NJ, WAC6503D-S, WAC6502D-S, WAC6502D-E, WAC6553D-E, WAC6103D-I			—
Макс. кол-во управляемых точек доступа (базовая комплектация/с лицензией)	2/34	2/66	2/66	—
Поддержка радиоинтерфейсов 2,4 ГГц и 5 ГГц	Да	Да	Да	—
Встроенный интерфейс WLAN				
Поддерживаемые стандарты сетей Wi-Fi	—	—	—	—
Радиоинтерфейс 2,4 ГГц	—	—	—	—
Радиоинтерфейс 5 ГГц	—	—	—	
Безопасность				
Межсетевой экран (SPI Firewall)	Да	Да	Да	Да
Поддержка IPSec VPN	Да	Да	Да	Да
Поддержка SSL VPN	Да	Да	Да	Да
Поддержка L2TP/IPSec VPN	Да	Да	Да	Да
Антивирус (AV)	Да	Да	Да	Да
Предотвращение вторжений (IDP)	Да	Да	Да	Да
Патруль приложений (AP)	Да	Да	Да	Да
Фильтрация веб-контента (CF)	Да	Да	Да	Да
Фильтрация спама (AS)	Да	Да	Да	Да
Инспектирование SSL	Да	Да	Да	—
Резервирование				
Резервирование и балансировка нагрузки WAN	Да	Да	Да	Да
Резервирование и балансировка нагрузки IPSec VPN	Да	Да	Да	резервирование
Резервирование устройства (Device HA)	Да	Да	Да	Да
Аутентификация пользователей				
Локальная база данных	Да	Да	Да	Да
RADIUS	Да	Да	Да	Да
Прозрачная аутентификация пользователей MSAD (Single Sign-On)	Да	Да	Да	—
Администрирование				
Графический веб-интерфейс (HTTP и HTTPS)	Да	Да	Да	Да
Командная строка (SSH, Telnet)	Да	Да	Да	Да
ZyXEL One Network (ZON)	Да	Да	Да	—
Vantage Report	Да	Да	Да	Да
Физические характеристики				
Габариты, мм (Ш x Г x В)	430 x 250 x 44	430 x 250 x 44	430 x 250 x 44	430 x 487 x 89
Масса, кг	3,30	3,30	3,30	10,50

Дополнительное программное обеспечение и принадлежности

ZyWALL IPSec VPN

Программный VPN-клиент для безопасного удаленного доступа на основе IPSec, совместимый со всеми моделями ZyWALL и ZyWALL USG.

Vantage CNM for Windows

Программный комплексный инструмент централизованного управления и мониторинга устройств сетевой безопасности ZyXEL.

Vantage Report 3.3

Программный инструмент для быстрого и удобного централизованного сбора, хранения, анализа и обработки информации о работе распределенной сети устройств безопасности ZyXEL.

Cloud CNM

Cloud CNM — облачная система централизованного управления межсетевыми экранами ZyWALL и центрами безопасности USG.

Лицензии для подключения дополнительных функций и услуг

	USG20/20W-VPN	USG 40/40W	USG 60/60W	ZyWALL 110	ZyWALL 310	ZyWALL1100	USG 1900
Антивирус	—	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года
IDP/AP	—	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года
Фильтрация веб-контента	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года
Антиспам	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года	1/2 года
Антивирус+IDP/AP +фильтрация веб-контента+антиспам	—	1 год	1 год	1 год	1 год	1 год	1 год
Vantage CNM	—	—	—	—	—	—	—
Vantage Report	Поддержка всех моделей, 1 устройство, 5 устройств, 25 устройств, 100 устройств						
Cloud CNM	Поддержка всех моделей						
Управление точками доступа Wi-Fi	+4/+8 дополнительных точек						
Device HA Pro	—	—	—	Да	Да	Да	Да
Hotspot Management	—	—	—	—	1год / постоянная		
Туннели SSL VPN	+5/+10 туннелей	+5/+10 туннелей	+5/+10 туннелей	+5/+10/+50 туннелей			
ZyWALL IPSec VPN Client	Для клиентских компьютеров под управлением Windows: 1,5,10,50 инсталляций						
SecuExtender SSL VPN Client	Для клиентских компьютеров под управлением Mac OS X: 1,5,10 инсталляций						

	USG 2000
Антивирус	1/2 года
IDP/AP	1/2 года
Фильтрация веб-контента	1/2 года
Антиспам	1/2 года
Vantage CNM	Поддержка всех моделей, 10 узлов, 25 узлов, 50 узлов, 100 узлов, 300 узлов, 1000 узлов
Vantage Report	Поддержка всех моделей, 1 устройство, 5 устройств, 25 устройств, 100 устройств
Cloud CNM	—
Управляемые точки доступа Wi-Fi	—
Туннели SSL VPN	5–50, 5–250, 5–750, 50–250, 50–750, 250–750
ZyWALL IPSec VPN Client	Для клиентских компьютеров: 1,5,10,50 инсталляций
SecuExtender SSL VPN Client	—

ZyXEL Беларусь
220123, Минск,
ул. В. Хоружей, 32а, офис 26
http://zyxel.by
+375 (17) 334-6099

ZyXEL Россия
117437, Москва,
ул. Островитянова, 11, корпус 1
http://zyxel.ru
(495) 539-9935

ZyXEL Украина
04050, Киев,
ул. В.Черновола, 12, БЦ «Лекс»
http://zyxel.ua
(044) 494-4931

ZyXEL Центральная
Азия и Закавказье
050010, Казахстан,
Алматы, пр. Достык, 43, офис 205
http://zyxel.kz
+7 (727) 259-0699