УНИВЕРСИТЕТ ИТМО

С.М. Платунова,
И.В. Елисеев,
Е.Ю. Авксентьева

РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ. ШЛЮЗ БЕЗОПАСНОСТИ КАК УНИВЕРСАЛЬНОЕ СРЕДСТВО ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Санкт-Петербург
2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

С.М. Платунова,
И.В. Елисеев,
Е.Ю. Авксентьева

РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ. ШЛЮЗ БЕЗОПАСНОСТИ КАК УНИВЕРСАЛЬНОЕ СРЕДСТВО ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО

по направлению подготовки 09.04.01 Информатика и вычислительная техника 09.03.01 Информатика и вычислительная техника, 27.04.04 Управление в технических системах, 27.03.04 Управление в технических системах в качестве учебно-методического пособия для реализации основных образовательных программ магистратуры и бакалавриата.

Санкт-Петербург
2020

Платунова С.М., Елисеев И.В., Авксентьева Е.Ю., Реализация комплексной безопасности в корпоративных сетях. Шлюз безопасности как универсальное средство для обеспечения защиты данных и предотвращения вторжений.– СПб: Университет ИТМО, 2020. – 64 с.

Рецензент(ы):
Жуков Николай Николаевич, кандидат физико-математических наук, , доцент (квалификационная категория "доцент практики") факультета программной инженерии и компьютерной техники, Университета ИТМО.

В учебно-методическом пособии описаны вопросы реализации комплексной безопасности в корпоративных сетях на основе шлюза безопасности, как универсального средства для обеспечения защиты данных и предотвращения вторжений.
Учебно-методическое пособие предназначено для подготовки магистров по направлению 09.04.01 Информатика и вычислительная техника, 27.04.04 Управление в технических системах, и бакалавров по направлению 09.03.01 Информатика и вычислительная техника, 27.03.04 Управление в технических системах.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Введение

В пособии рассматриваются универсальные шлюзы безопасности на примере устройств фирмы ZyXEL, которые применяются для обеспечения безопасности вычислительных систем и сетей и комплексной защиты данных в корпоративных компьютерных сетях.

Тема 1. Обзор оборудования

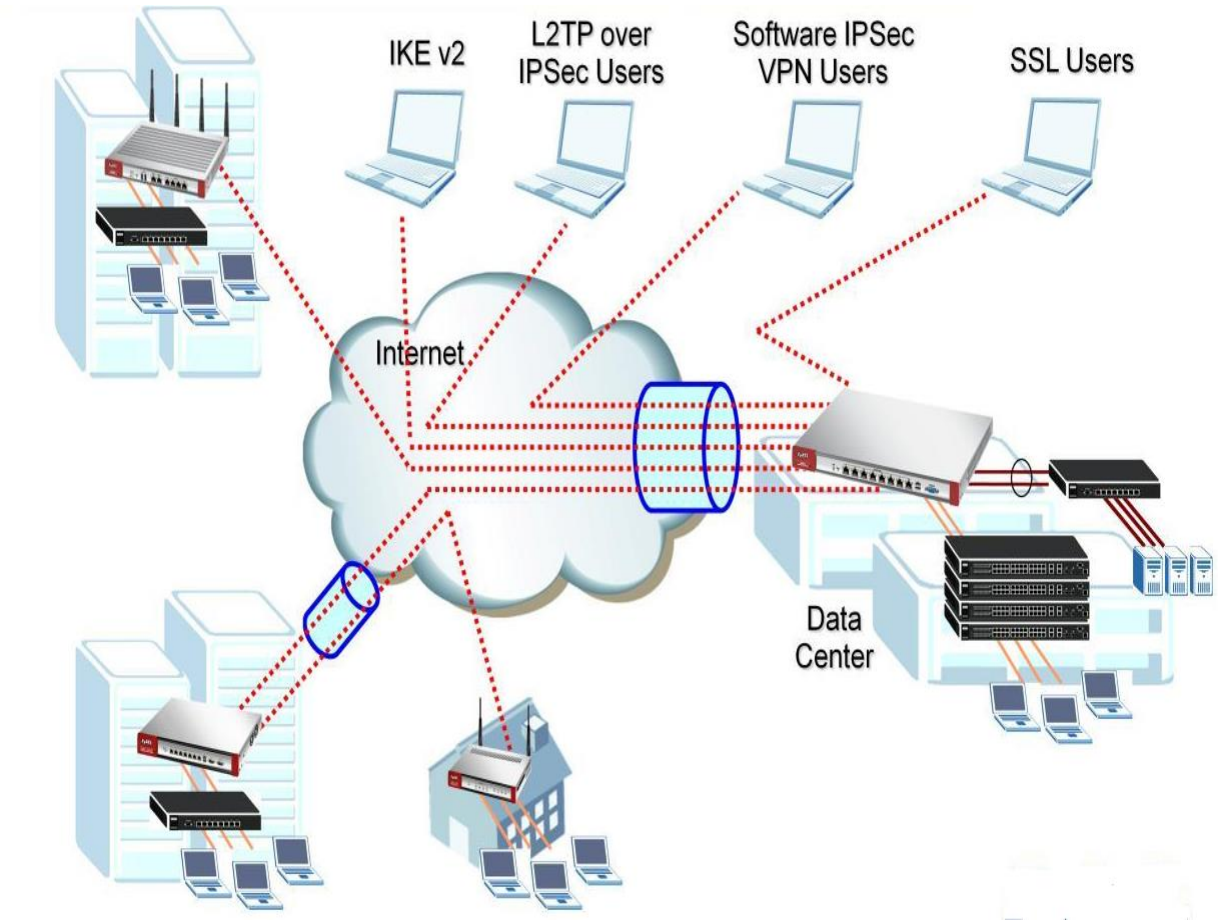


Рис. 1. Пример корпоративной распределённой сети

Универсальные шлюзы безопасности поддерживают:

1. технологии VLAN и виртуальные интерфейсы.
2. такие функции как:
   - IPsec,
   - L2TP/IPsec VPN и
   - SSL VPN виртуальных частных сетей.
3. ZyXEL ZyWALL и USG может также быть применен в роли VPN-концентратора, для объединения территориально распределенных

объектов в единую сеть или создания мобильных удаленных рабочих мест.

4. осуществляют резервирование доступа в Интернет и балансировку нагрузки.
5. осуществляют подключения к провайдеру с помощью USB модемов 2,5/3G/4G.
6. Инструментарий управления полосой пропускания шлюзов позволяет вводить приоритеты передачи трафика, гарантируя либо ограничивая использование доступной емкости подключения для определенных типов трафика или хостов в сети.
7. У универсальных шлюзов безопасности имеется встроенная поддержка работы с функциями LDAP/MS AD/RADIUS.

На рис. 1 показан пример сети с использованием функций шлюзов безопасности ZyWALL и USG.

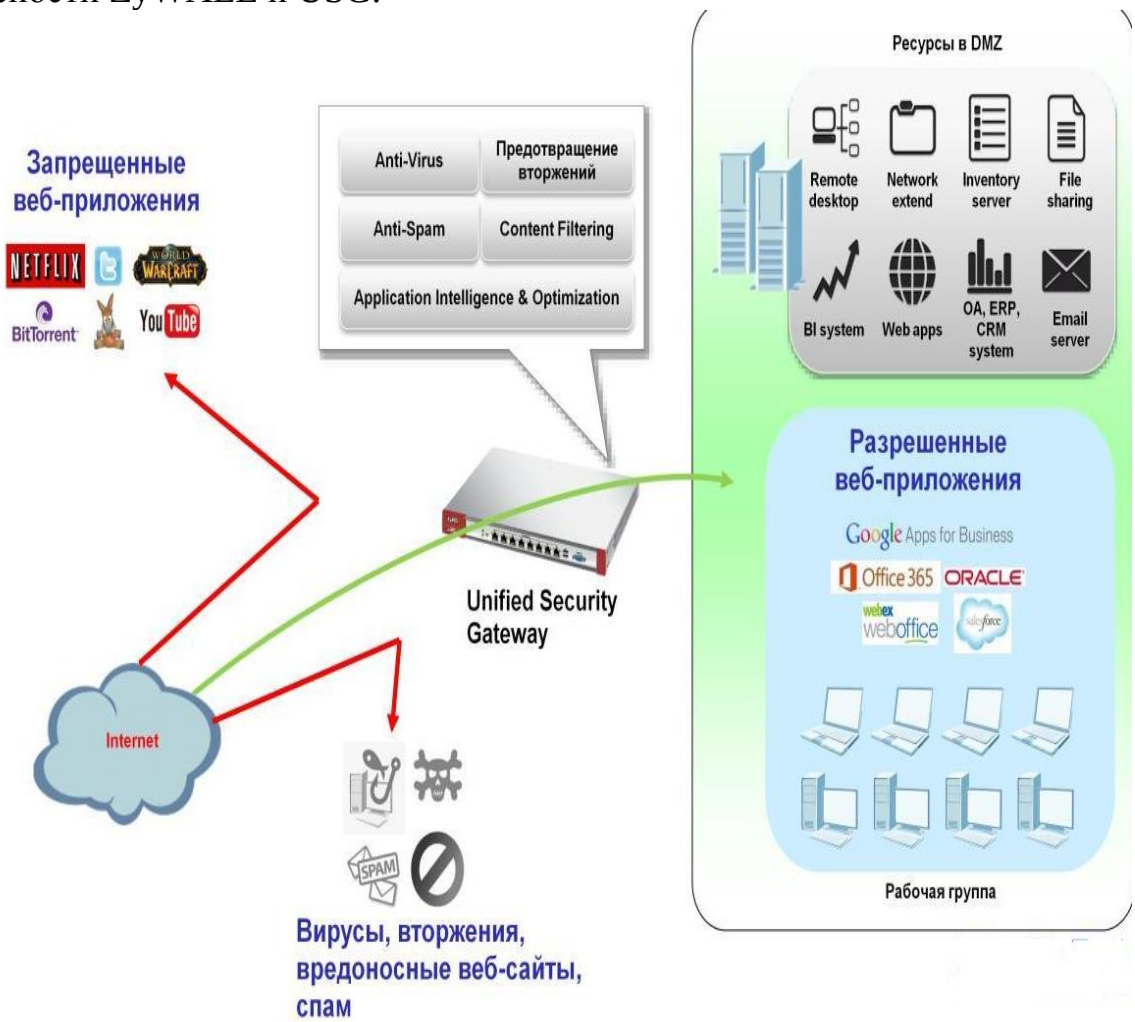


Рис. 2. Модель угроз

Шлюз ZyXEL ZyWALL или USG предназначен для решения всего комплекса задач сетевой безопасности, включает функциональную настраиваемую защиту от вирусов и спама, управление шириной полосы пропускания для разнообразных объектов сети, контроль трафика приложений, предотвращение вторжений и виртуальные частные сети.

Помимо межсетевого экрана и механизма NAT, шлюзы серии ZyXEL ZyWALL или USG имеют:

1. встроенный антивирус,
2. службы обнаружения и предотвращения вторжений IDP
3. выявления аномалий протоколов ADP.

Устройство способно предотвращать разнообразные атаки вплоть до 7 уровня OSI на основе:

1. использования обновляемых баз данных сигнатур,
2. проверки состояния пакетов,
3. определения моделей поведения и многих других современных методик.

На рис. 2 показана модель угроз, которым подвергаются данные, передаваемых корпоративной сетью, и возможности универсальных шлюзов безопасности

Устройства ZyXEL ZyWALL и USG

Межсетевые экраны ZyXEL: USG ZyWALL с функциями VPN вошли в модельный ряд устройств сетевой безопасности для малых и средних предприятий.

Эти устройства предназначены для решения задач по созданию высокоскоростных защищенных каналов передачи данных через Интернет для связи с удаленными офисами, филиалами, партнерами и выездными сотрудниками, отвечая тенденциям малого и среднего бизнеса к глобализации и мобильности бизнес-процессов.

Устройства ZyXEL ZyWALL и USG демонстрируют одни из самых высоких показателей пропускной способности SPI Firewall и VPN в своем классе устройств.

Высокая производительность новых устройств серии ZyWALL и USG делает их оптимальным решением для малых и средних предприятий с уже сформированной защитой от угроз из Интернета, предъявляющих повышенные требования к скорости и надежности связи с удаленными филиалами, партнерами и сотрудниками. Характеристики шлюзов безопасности серии USG показаны ниже.

1. Количество VPN во всех устройствах фиксировано.
2. Функция Device-HA присутствует в устройствах, начиная с ZyWALL USG 110.
3. Firewall: максимальная производительность вычисляется на основе RFC 2544 (UDP пакеты, 1518 байт).
4. VPN (AES): пропускная способность измеряется с использованием UDP трафика с размером пакета 1424 байт, вычисляется на основе RFC 2544.
5. UTM (AV + IDP) пропускная способность, измеренная с помощью стандартных тестов IXIA IxLoad, используется HTTP протокол с

размером пакета 1460 байта. Испытания проводились с несколькими потоками.

6. Максимальная пропускная способность вычисляется на основе RFC 2544, реальная пропускная способность может изменяться в зависимости от конфигурации, состояния сети и активированных услуг.

Управление шлюзами безопасности

Управление шлюзами безопасности ZyWALLи USG включает в себя пять способов управления HTTP, RS-232, Telnet/SSH, SNMP, FTP. Все сетевые службы управления могут быть отключены в случае необходимости. Для всех сетевых служб также можно изменить номер порта. В зависимости от способа управления будут доступны различные настройки. Можно включить или выключить протокол управления, изменить стандартный номер порта, настроить политику доступа относительно зон.

Аутентификация

ZyWALL и USG поддерживает несколько учетных записей администраторов, а также учетные записи пользователей.

Учетные записи можно объединять в группы, и при настройке различных функций указывать, для какого пользователя или группы пользователей данная функция будет работать.

Например, можно настроить так, что пока пользователь не пройдёт аутентификацию + авторизацию на ZyWALL, он не сможет иметь доступ к определенным серверам, например, почтовый сервер, файловый сервер, маршрут во внешнюю сеть и т.д.

Пользователи ldap-users, radius-users, ad-users являются служебными. Они служат для аутентификации пользователя в соответствующей базе данных. В дальнейшем их можно использовать в различных правилах (маршрутизации, доступа и т.д.). В таком случае политика, настроенная в таком правиле будет применима относительно всех пользователей выбранной группы. Так же можно создавать такие политики для конкретного внешнего пользователя (ext-user) или сразу для конкретной группы, присутствующей в базе данных, создав группового пользователя (ext-group-user).

ZyWALL USG поддерживает 5 типов учетных записей:

1. **Admin** — привилегии уровня Admin позволяют менять любые настройки на ZyWALL
2. **Limited-Admin** — привилегии уровня Limited-Admin позволяют просматривать любые настройки на ZyWALL, однако из исполняемых команд будет доступна лишь малая часть, которая относится к диагностике устройства.
3. **User** — привилегии уровня User позволяют получать доступ к службам сети, а также просматривать список команд CLI на ZyWALL

4. **Guest** — привилегии уровня Guest позволяют получать доступ к службам сети
5. **Ext-User** — данный тип пользователей может получать доступ к различным службам сети, однако аутентификация этих пользователей проходит на внешнем сервере аутентификации (AD, LDAP, RADIUS).
6. **Ext-group-user** – аутентификация пользователей входящих в определенную группу на внешнем сервере аутентификации (AD, LDAP, RADIUS).

Создание пользователя производится в меню configuration> object> user/group> user.

Настройка авторизации через Active Directory показан на рис. 3.

Рассмотрим схему, в которой используется аппаратный шлюз серии ZyWALL, и к нему подключен сервер MS Active Directory (AD), имеющий IP-адрес 192.168.1.222 (в нашем примере используется AD из состава ОС Windows Server 2003).

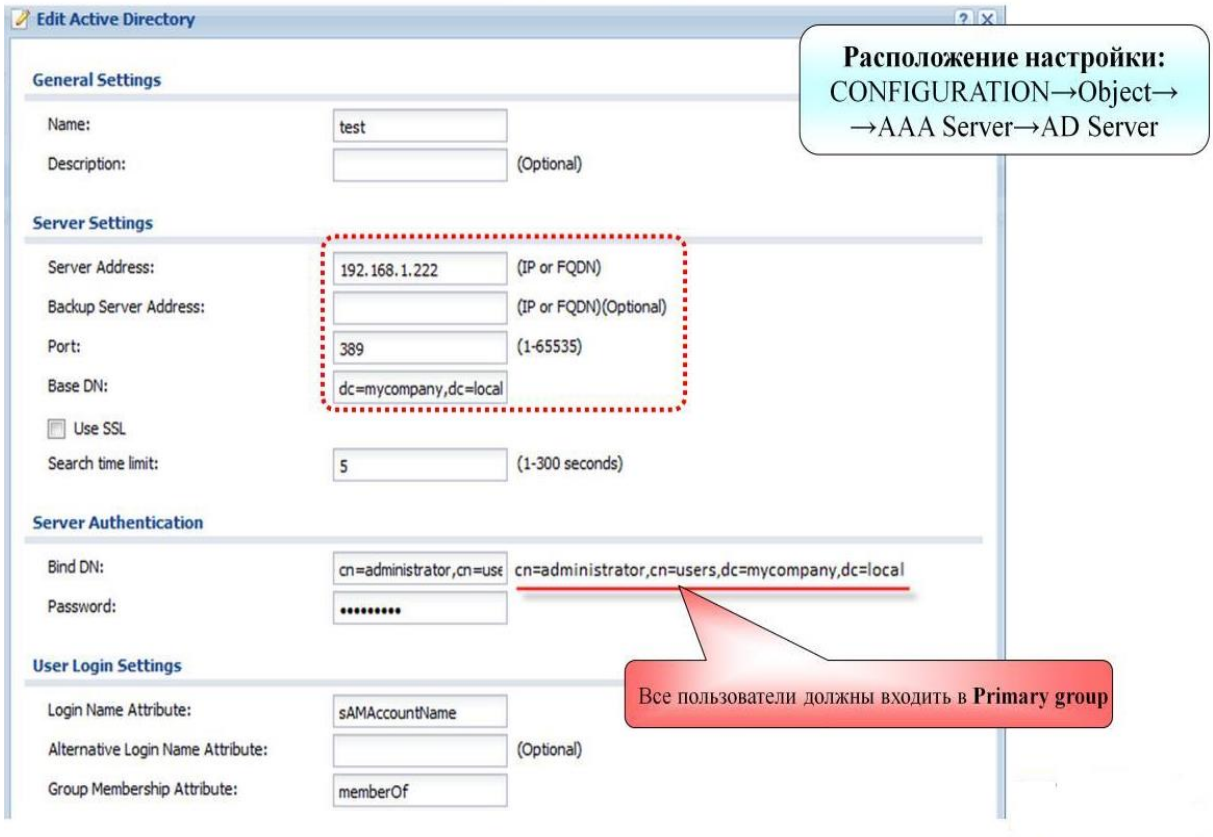


Рис. 3. Настройка авторизации через Active Directory

В Active Directory создан тестовый домен mycompany.local. В него входит контейнер Users, в котором находятся все пользователи и группы.

Пользователь для аутентификации в AD: administrator

Пароль: admin**** (Domain administrator’s password)

Используется CN Identifier: sAMAccountNAME

В разделе Configuration Validation можно проверить подключение к ADсерверу, попытавшись авторизовать существующего пользователя на сервере.
Все пользователи домена должны входить в общую группу, которая является основной (Primary group). В этом случае USG сможет распознать принадлежность пользователя к группам. Если Primary group отсутствует или основной назначена рабочая группа, она не будет распознана на USG.
Кириллицу нельзя использовать ни в какой кодировке в именах при настройке параметров Active Directory. Пример рабочей записи:
CN=ivanovinavivanovich,OU=IT,DC=domainname,DC=local
Используемый в примере пользователь (рис. 4) vasy входит в группу Programmers, созданную на сервере AD (Active Directory).

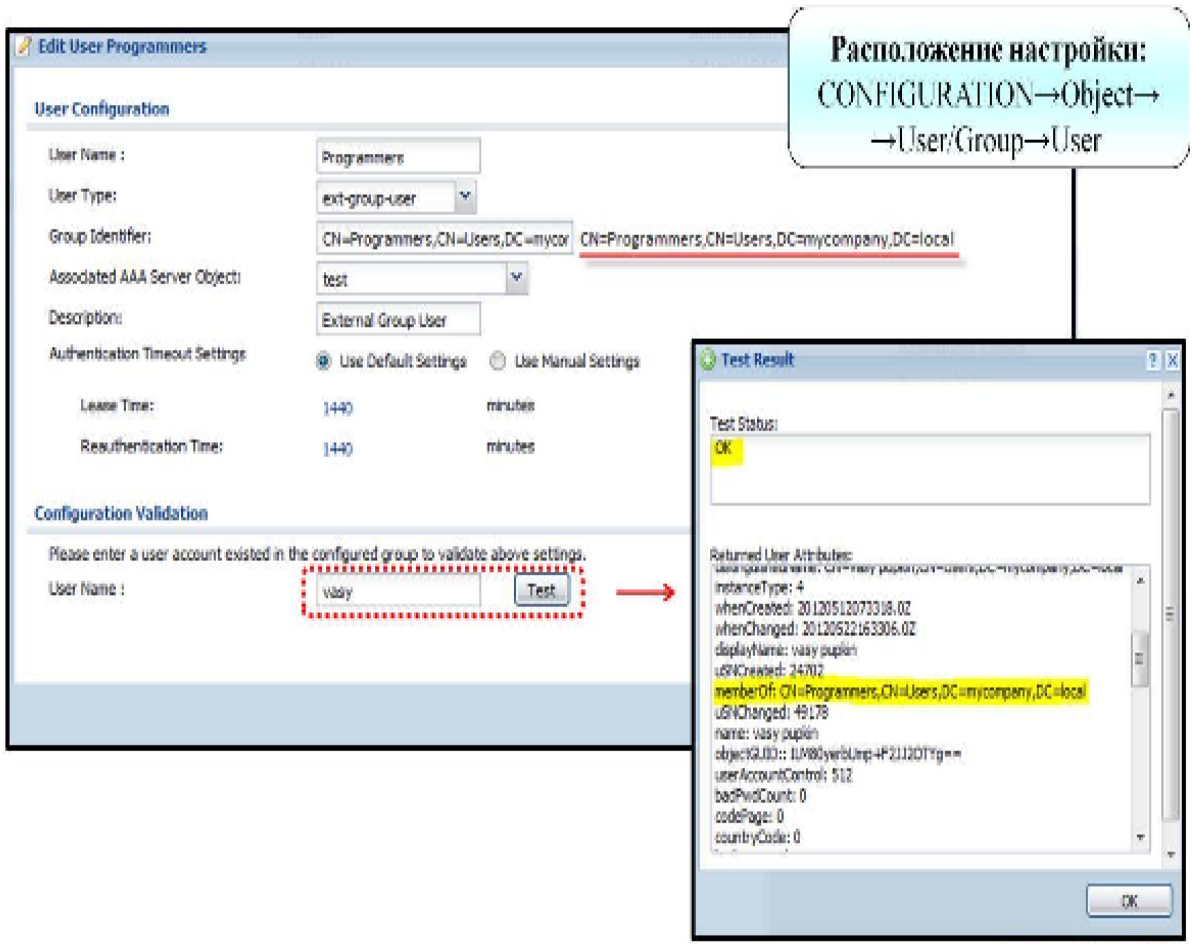


Рис. 4. Создание группового пользователя

В разделе Configuration Validation можно проверить подключение к ADсерверу и принадлежность пользователя к группе. Если пользователь принадлежит к данной группе, в поле Test Status будет значение OK.
Как видно из нашего примера, пользователь vasy принадлежит к группе Programmers (рис. 4).
Это отображается в поле Returned User Attributes в строке memberOf.
Обратим внимание на синтаксис указания идентификатора группы (Group Identifier). Нужно учитывать регистр букв. CN(контейнер) нужно указывать прописными буквами!

Механизм аутентификации пользователей Single Sign-on (SSO) и выше допускает прозрачную аутентификацию пользователей MS AD (Active Directory) на устройствах ZyWALL или USG.
При этом контроллер домена АД и агент SSO могут быть установлены на одном сервере.
Программа SSO, установленная на одном сервере с контроллером домена или отдельно стоящем сервере, осуществляет взаимодействие между контроллером домена и устройством ZyWALL, передавая на ZyWALL данные о пользователе при входе в домен и выходе из домена.
С прозрачной аутентификацией SSO пользователю домена не требуется дополнительно вводить свой логин и пароль для аутентификации на ZyWALL.
Будучи авторизованным контроллером домена, он будет автоматически авторизован устройством ZyWALL с применением соответствующих политик безопасности, сконфигурированными IT-персоналом, администрирующим устройство.

Управление посредством WEB GUI

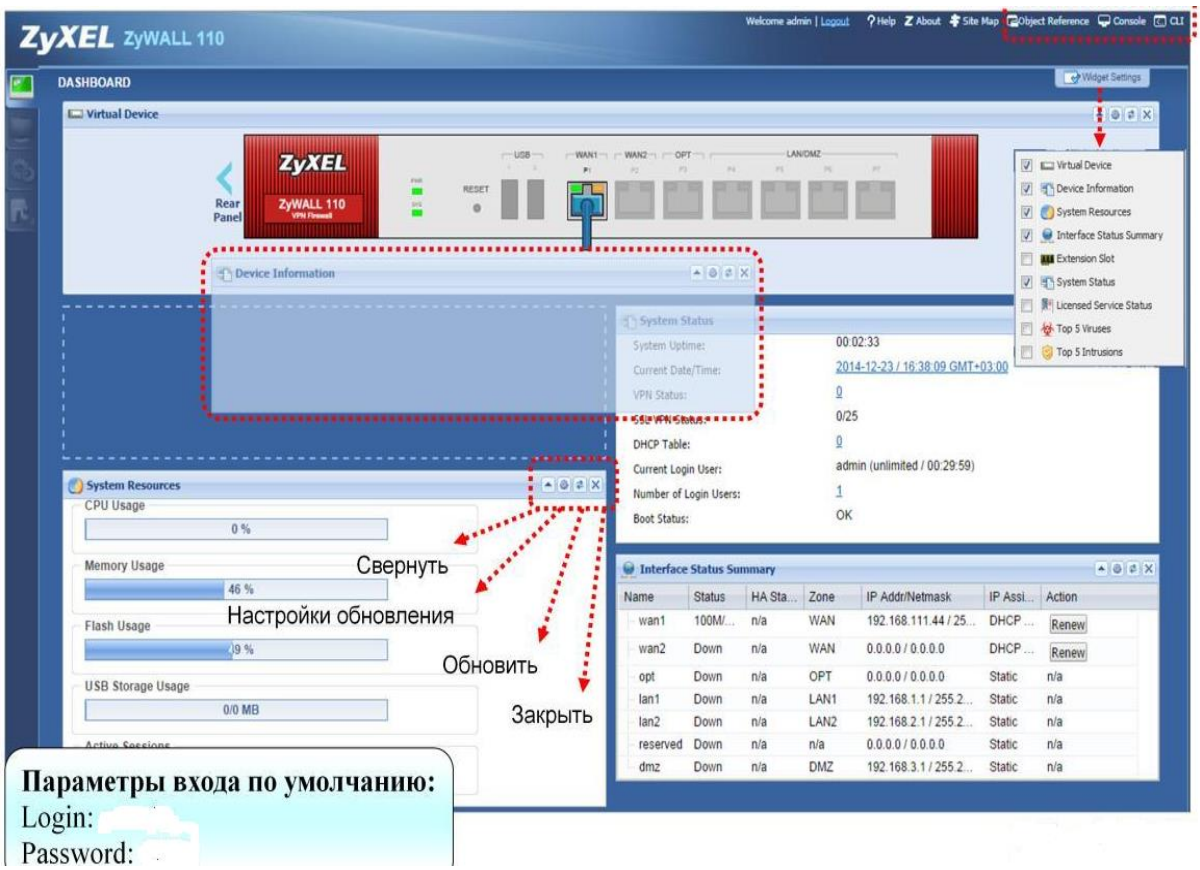


Рис. 5. Dashboard

GUI устройств является очень гибким и настраиваемым. Каждый блок работает как независимый виджет (рис. 5).
Up Arrow – позволяет свернуть виджет.
Refresh time setting – позволяет настроить интервал автоматического обновления виджета.

Refresh now – обновления виджета по нажатию. Close this widget – закрыть виджет.
В меню widget settings можно включить/выключить виджеты.
Виджеты можно расположить в нужном порядке.
Для этого нужно выбрать виджет и перетащить его в нужное место.
С помощью Object Reference на главной странице Dashboard можно выбрать тип объекта и название объекта, а затем, нажав кнопку "Обновить", получить список настроек относящихся к этому объекту.
Получить список связанных настроек к интересуемому объекту можно как на главной странице GUI устройства, так и непосредственно на странице конфигурации данного объекта.

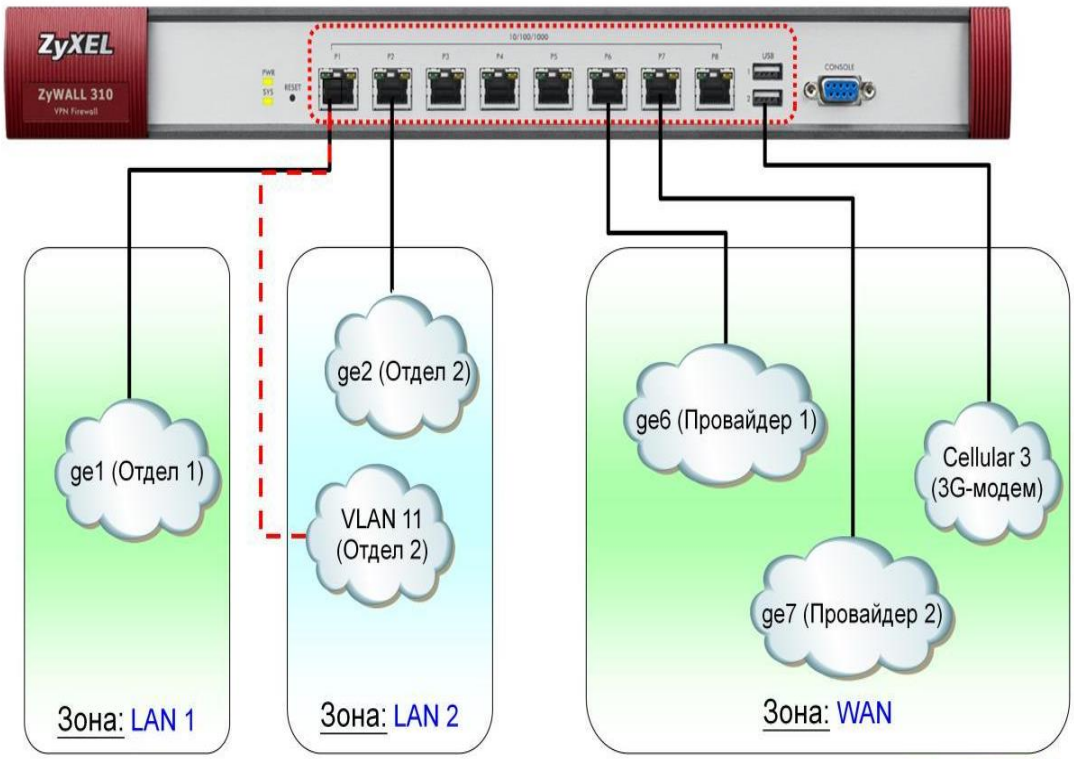


Рис. 6. Логика настройки интерфейсов портов зон

USB- Storage

GUI устройства позволяет сохранять log-файл и другую диагностическую информацию на USB-накопитель.
Для этого в GUI устройства достаточно включить функцию и указать желаемый максимальный предел от объема накопителя в мегабайтах или процентах.
Настройка расположена в меню CONFIGURATION> System> USB Storage.

Интерфейсы

Порты

В устройствах ZyWALL и USG физическим портам сопоставляются интерфейсы, которые далее объединяются в зоны.

Начиная с ZyWALL 310, интерфейсы, входящие в зону можно изменять, а также удалять из зоны.
Логика настройки интерфейсов портов зон показана на рис. 6.
В младших моделях в зоны можно только добавлять незадействованные или самостоятельно созданные интерфейсы такие как bridge или VLAN.
Соответствующая настройка в меню шлюза безопасности показана на рис. 7 (CONFIGURATION> Interfaces> Port role).
В младших моделях ZyWALL и USG после настройки предопределенных интерфейсов они назначаются на физические порты, с некоторыми отличиями.
В младших моделях ZyWALL и USG с двумя WAN – портами, 1-й и 2-й порт могут быть только WAN интерфейсами, 3-6-й порты могут быть LAN\DMZ интерфейсами.
Настройка Ethernet интерфейсов.
В младших моделях серии ZyWALL и USG определено несколько Ethernet интерфейсов, их тип и количество зависит от модели устройства.
В старших версиях ZyWALL все интерфейсы равноценны и не предопределены.

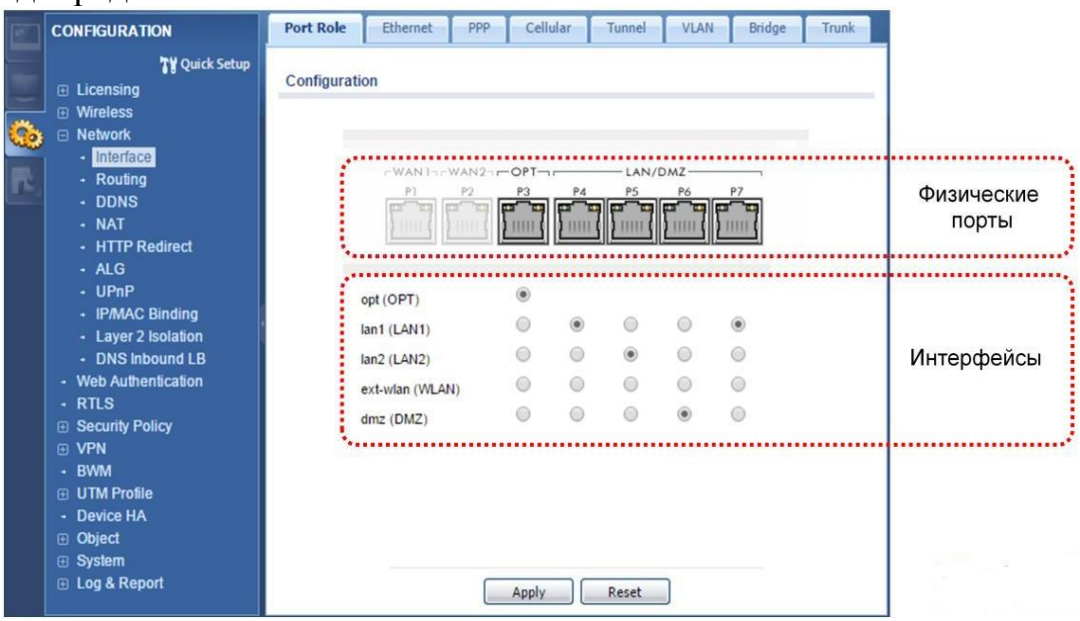


Рис.7. Роль порта / группировка портов

Зоны

Понятие «зоны» на всех устройствах серии ZyWALL и USG абсолютно одинаково и подразумевает под собой группы интерфейсов. Интерфейсы объединяются в зоны (группы), и именно эти зоны впоследствии используются для настроек различных политик, функций безопасности и т.д.
С точки зрения настройки различие между младшими устройствами серии ZyWALL и старшими заключается лишь в том, что на младших устройствах все зоны предопределены и возможно только изменять существующие зоны и нет возможности добавлять новые, на старших же устройствах количество и имена зон не определены.

Членом группы может быть любой из нижеперечисленных интерфейсов:

1. Ethernet
2. VLAN
3. Bridge
4. PPPoE/PPTP
5. Аналоговый модем
6. VPN туннель

Виртуальные интерфейсы автоматически включаются в ту же зону, куда включен первичный интерфейс.

При настройке любой зоны необходимо не только выбрать членов данной зоны, но и определить, возможна ли передача трафика между членами данной зоны, за это отвечает функция Block Intra-Zone Traffic.

Типы и Настройка интерфейсов

В устройствах ZyWALL и USG существует три типа (рис. 8) интерфейсов: internal, external и general.

Для некоторых USG ZyWALL 110 тип интерфейса является фиксированным.

Для некоторых ZyWALL тип интерфейса может быть настроен. По умолчанию, все интерфейсы general.

В зависимости от выбранного типа интерфейса будут поддерживаться те или иные функции, и меню его настройки будет отличаться.

Тип интерфейса	Internal	External	General
Модель устройства	USG 20/20W, 40/40W, 60/60W, ZyWALL 110: LAN1, LAN2, DMZ	USG 20/20W, 40/40W, 60/60W, ZyWALL 110: WAN1,WAN2	ZyWALL 310/1100: ge1,ge2,ge3,ge4.ge5... ZyWALL 110, USG 40/40W : OPT port **Все модели: VLAN, bridge**
DHCP Клиент	-	+	+
DHCP Сервер	+	-	+
DHCP Relay	+	-	+
Шлюз по умолчанию	-	+	+
Метрика	-	+	+
Проверка Ping	-	+	+
Смена MAC	-	+	+

Рис.8. Типы интерфейсов

Настройка внутреннего интерфейса находится в меню CONFIGURATION> Network> Interface> Ethernet.

Внутренний тип интерфейса предназначен для подключения к локальной сети.

Когда выбран тип internal, то интерфейс не может работать в качестве клиента DHCP, а может работать только в качестве сервера DHCP и DHCP relay.

Настройка внешнего интерфейса находится в меню CONFIGURATION> Network> Interface> Ethernet

Внешний тип интерфейса служит для подключения к внешней сети (например, Интернет).

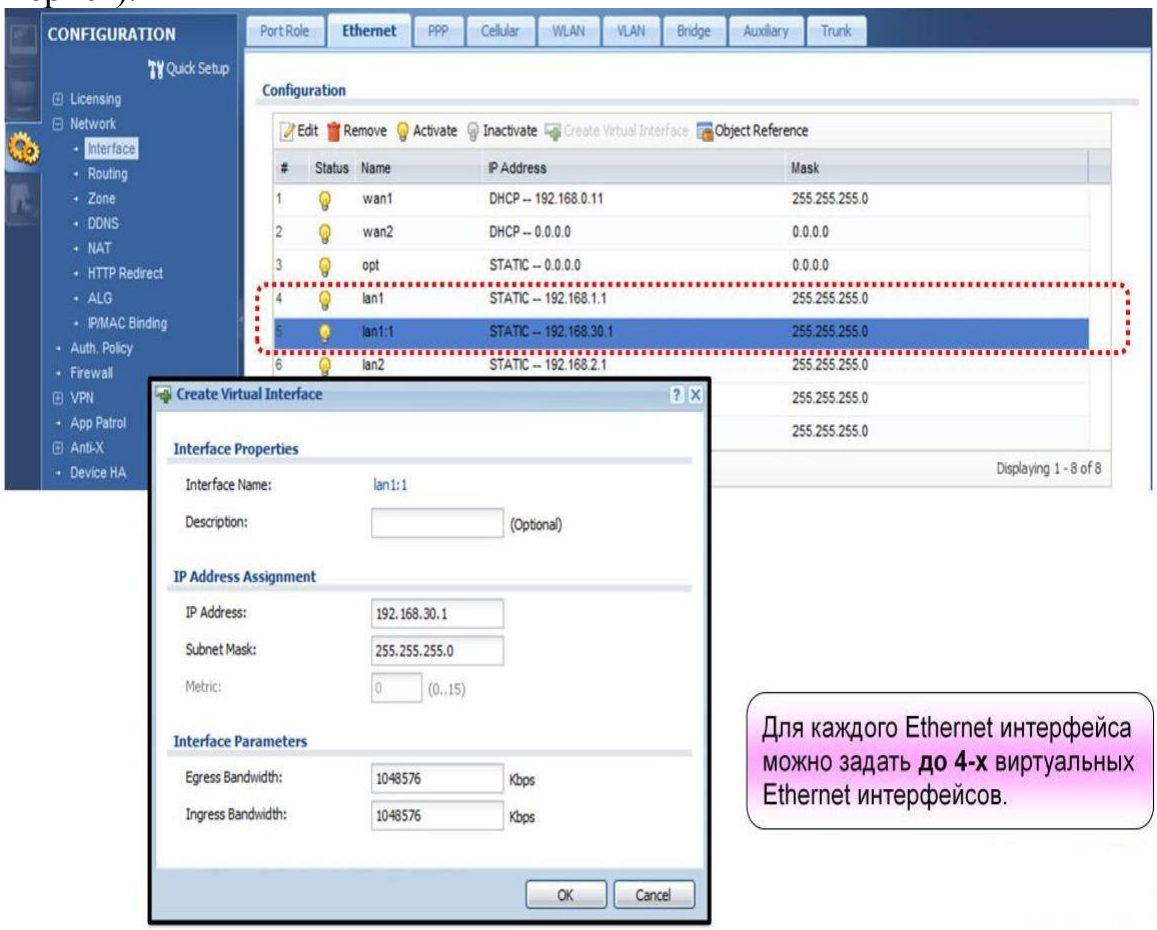


Рис.9. Виртуальные Ethernet интерфейсы

Когда выбран тип external, интерфейс может работать только в качестве клиента DHCP без других функций DHCP. В этом режиме можно установить метрику и параметры проверки подключения. Имя Ethernet и PPP интерфейса может быть изменено на значимые или практические имена интерфейсов. Изменение названия интерфейса будет автоматически применяться во всех настройках, которые ссылаются на интерфейс.

Виртуальные Ethernet интерфейсы

ZyWALL USG и ZyWALL позволяет создавать виртуальные Ethernet интерфейсы (назначение нескольких подсетей на один Ethernet интерфейс).

Для каждого Ethernet интерфейса можно задать до 4 виртуальных Ethernet интерфейсов (рис. 9).

PPPoE PPTP интерфейсы

В младших моделях серии ZyWALL и USG предопределено три PPP интерфейса (рис. 10), которые соответствуют WAN1, WAN2 и OPT интерфейсам.

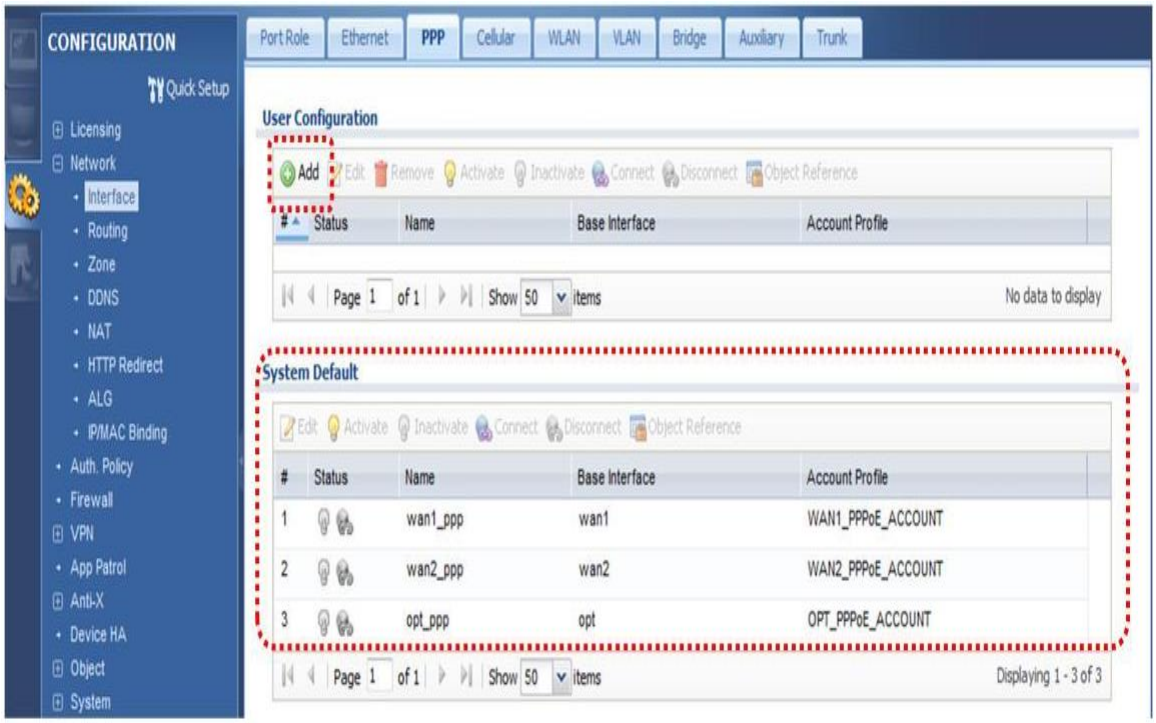


Рис. 10. PPPoE PPTP интерфейсы

В старших моделях серии ZyWALL, PPP интерфейсы не предопределены.

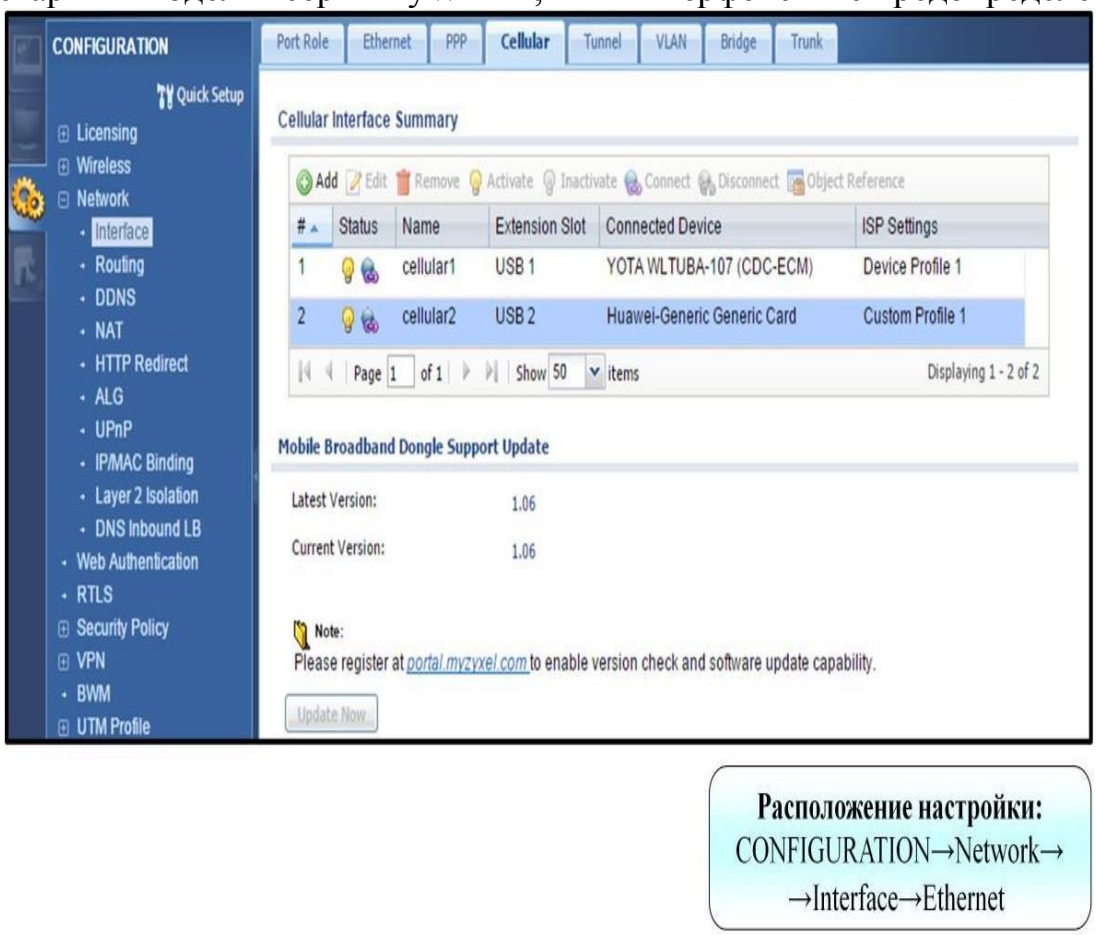


Рис. 11. Интерфейс сотовой связи

Возможности по настройке PPP интерфейсов между младшими моделями серий ZyWALL и старшими совпадают.
Настройка PPPoE PPTP интерфейсов находится CONFIGURATION> Network> Interface> PPP.
Встроенный клиент PPTP VPN имеет возможность адресовать сервер VPN не только IP-адресом, но и доменным именем, что позволяет устройствам ZyWALL нормально работать при PPTP-подключении к Интернет-провайдерам, использующим балансировку нагрузки серверов VPN, основанную на DNS.
ZyWALL и USG может выступать в роли клиента PPPoE или PPTP. Устройства ZyWALL и USG позволяют использовать CDMA 3G или 4G модемы для организации доступа в интернет через мобильных поставщиков услуг.

Интерфейс сотовой связи

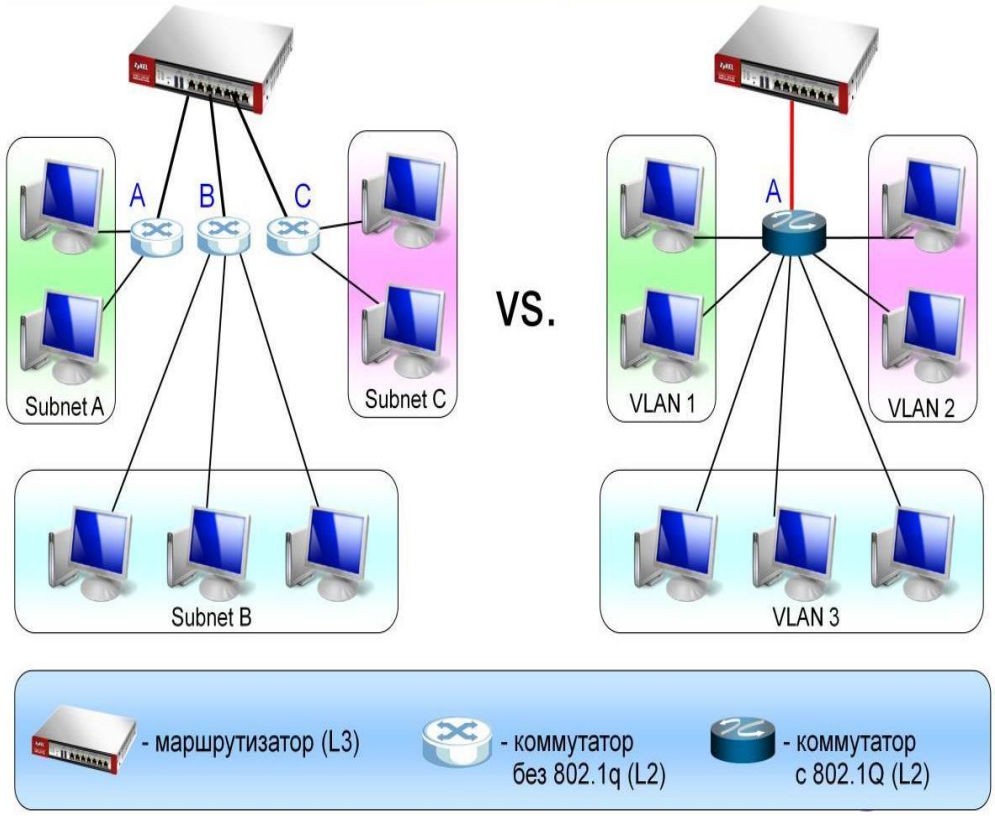
Интерфейс сотовой связи показан на рис. 11. Настройка интерфейса сотовой связи располагается в меню CONFIGURATION> Network> Interface> Ethernet.
Для интерфейса мобильного доступа в интернет через 3G или 4G модем можно задать ограничение использования соединения по времени и\или количеству трафика.
Это позволит избежать перерасхода, установленного тарифным планом лимита включенных часов или пакета трафика.
Для ряда модемов также потребуется задать такие параметры, как: APN-точка доступа, номер для дозвона и параметры для аутентификации.
Эти параметры можно узнать у вашего провайдера доступа к мобильному интернету.
Для разных регионов они могут отличаться.
После установления соединения с оператором появляется дополнительный интерфейс.
В статусе мобильного устройства всегда можно посмотреть его параметры, характеристики, уровень сигнала и другую полезную информацию.

VLAN (Virtual Local Area Network)

VLAN — механизм, который позволяет разделить одну физическую сеть на несколько логических. Механизм VLAN описан в стандарте 802.1Q.
Рассмотрим схему, изображенную на рис. 12 сначала без использования VLAN, затем с использованием VLAN:
В первом случае у нас есть 3 отдела компании, логически отделы компании мы хотим разделить друг от друга, соответственно разделяем наши отделы по различным IP подсетям и получаем:

1. трафик внутри отдела на 2 уровне коммутируется на устройстве A, B или C.
2. трафик между отделами передается через маршрутизатор
3. недостаточный уровень безопасности (В случае использования одного неуправляемого коммутатора для всех отделов сотрудник

отдела A может установить статический адрес из диапазона отдела B и получить доступ к ресурсам отдела B)

4. 

5. Рис. 12. VLAN интерфейсы

Во втором случае остается та же физическая есть, которую разделяем на 3 виртуальных локальных сети и получаем:

1. трафик внутри отдела на 2 уровне коммутируется на устройстве A
2. трафик между отделами передается через маршрутизатор
3. широковещательный трафик передается только внутри одного VLAN
4. повышенный уровень безопасности (даже если сотрудник отдела A установит статический адрес из диапазона отдела B, то доступ к ресурсам отдела он автоматически не получит, однако, сохраняется возможность доступа из отдела в отдел на основе маршрутизации через ZyWALL)
5. для каждого VLAN (отдела) можно назначить свои политики ограничения полосы пропускания, контентной фильтрации и т.д. Данные политики не зависят от физической структуры, то есть физическую сеть можно изменять, не меняя политик.

Интерфейс VLAN (Virtual Local Area Network) может выступать как в роли внутреннего (internal), внешнего (external), так и в роли настраиваемого (general) интерфейса.

Использование VLAN -интерфейсов позволяет увеличить количество логических интерфейсов, т.к. на физическом порту, в таком случае, может находиться сразу несколько VLAN интерфейсов.
При этом VLAN -интерфейсы будут работать совместно с обычными логическими интерфейсами (LAN1, LAN2 и т.д.).
Для работы такого интерфейса понадобится коммутатор второго, третьего уровня или L2+ уровня, способный в сторону ZyWALL передавать кадры в тегированном виде. Тегированный кадр увеличен на 4 байта относительно кадра без тега.

WAN trunk

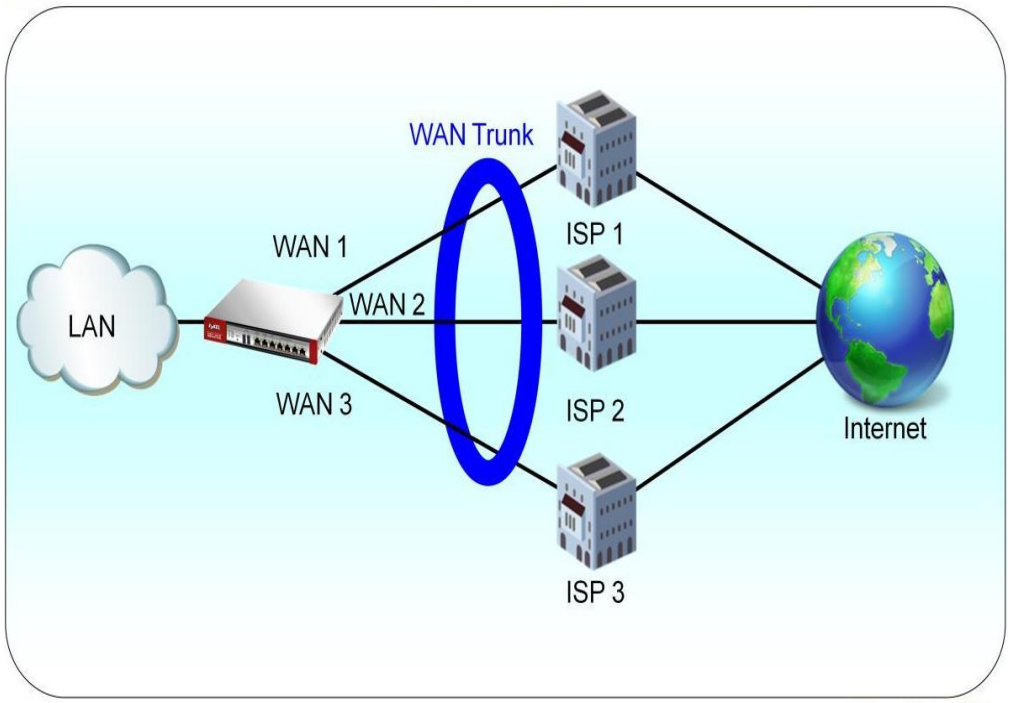


Рис.13. WAN trunk

WAN trunk — механизм, позволяющий объединять несколько внешних каналов в один логический транк, что позволит использовать несколько провайдеров доступа во внешнюю сеть одновременно (рис. 13).
Наиболее распространенное применение WAN транков — балансировка нагрузки и резервирование линии.
В младших моделях серии USG количество транков ограничено пятью, в старших моделях количество транков от 15 и более.
Для создания WAN Trunk необходимо определить членов данного транка, членом транка может являться любой интерфейс.
Далее необходимо выбрать режим работы каждого интерфейса, доступно два режима работы:

1. **Active** — активный интерфейс, то есть тот интерфейс, который ZyWALL будет использовать для передачи данных.
2. **Passive** — пассивный интерфейс, то есть тот интерфейс, который будет использоваться для передачи данных, только в том случае, если все active интерфейсы неработоспособны.

Количество пассивных интерфейсов в одном транке — не более одного.

После этого выбирается алгоритм балансировки нагрузки (рис. 14).

Алгоритмы балансировки нагрузки

Распределение нагрузки между интерфейсами в одном транке возможно по одному из 3 алгоритмов:

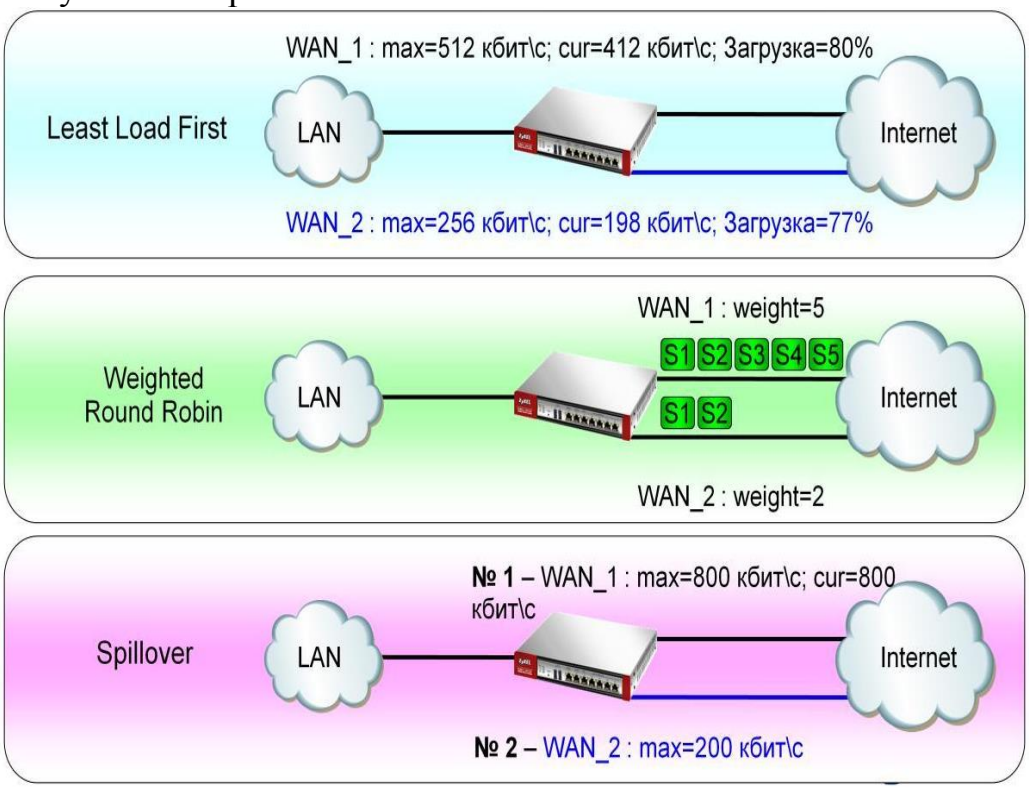


Рис. 14. Алгоритмы балансировки нагрузки

Алгоритм Least Load First

Алгоритм, при котором ZyWALL USG высчитывает процентную загрузку интерфейса относительно максимальной полосы пропускания данного интерфейса, причем в качестве нагрузки на интерфейс можно учитывать как входящий или исходящий трафик, так и оба потока одновременно.

Трафик новой сессии, который необходимо отправить, будет отослан в интерфейс с минимальной процентной загрузкой. Например, при наличии интерфейсов WAN_1 и WAN_2 с максимальной полосой пропускания 512 Kbps и 256 Kbps соответственно и текущей нагрузкой в 412 Kbps и 198 Kbps получаем:

1. процентная загрузка канала WAN_1 равна 412/512 = 0.8
2. процентная загрузка канала WAN_2 равна 198/256 = 0.77. Таким образом, данные новой сессии будут отправлены в интерфейс WAN_2, так как процентная загрузка данного канале наименьшая.

Алгоритм Weighted Round Robin

Алгоритм, основанный на весах интерфейсов. Для каждого интерфейса задается свой вес (число от 1 до 10), и, используя данные веса, ZyWALL и USG будет определять, в какой интерфейс отправлять данные новой сессии.
Например, при наличии интерфейсов WAN_1 и WAN_2 с весами 5 и 2 соответственно ZyWALL и USG будет отправлять по 5 сессий в интерфейс WAN_1 на каждые 2 сессии, отправленные через интерфейс WAN_2.
Алгоритм Spillover
Алгоритм, при котором для каждого интерфейса, включенного в WAN trunk, задается пороговое значение скорости.
Данные каждой новой сессии будут отправляться в тот интерфейс, на котором пороговое значение скорости не достигнуто, и этот интерфейс имеет наименьший порядковый номер в данном транке.
Например, при наличии интерфейсов WAN_1 и WAN_2 с ограничениями 800 Kbps и 200 Kbps соответственно, данные через интерфейс WAN_2 пойдут только в том случае, если интерфейс WAN_1 полностью загружен.

Маршрутизация

В шлюзах безопасности ZyWALL и USG имеется возможность настроить статические и динамические маршруты.
При этом политика маршрутизации Policy route позволяет отменить (аннулировать) автоматически созданный VPN route.
ZyWALL и USG поддерживает два типа статической маршрутизации:
Static Route — маршрутизация на базе подсети назначения
Policy Route — маршрутизация на базе расширенного набора критериев
Правила маршрутизации Policy Route имеют больший приоритет, нежели правила Static Route, то есть сначала проверяется, подходит ли данный пакет под действие какого-либо правила Policy Route, и только если ни под одно правило данный пакет не попал, то выбор маршрута будет определятся с помощью Static Route.
Policy Route — политики маршрутизации, позволяют создавать правила маршрутизации, основывающиеся не только на базе подсети назначения, но и на ряде других критериев.
Политики маршрутизации также применяются для управления полосой пропускания, при этом управление полосой пропускания в политиках маршрутизации имеет больший приоритет, нежели управление полосой пропускания в меню Application Patrol. При создании политик заполняют следующие поля.
User — пользователь или группа пользователей, для которых будет применяться данная политика маршрутизации
Incoming — входящий канал, в качестве входящего канала может быть любой интерфейс, VPN туннель, SSL соединение
Source Address — адрес источника (хост, подсеть, диапазон адресов)
Destination Address — адрес назначения (хост, подсеть, диапазон адресов)

Service — служба, трафик которой будет обрабатываться данной политикой (TCP/UDP порт, номер протокола IP)
Next-Hop Type — тип и имя следующего узла по пути следования пакета (шлюз, VPN туннель, wan trunk, интерфейс)
Address Translation — настройки функции NAT для данной политики маршрутизации. Данная функция не работает в случае, если в качестве следующего узла был выбран VPN туннель, так как для VPN соединений NAT настраивается при создании туннеля.
Healthy Check — механизм в Policy Routing, позволяет контролировать доступность маршрута, описанного правилом Policy Routing, путем пингования определенного хоста по соответствующему маршруту. В случае недоступности маршрута он исключается из таблицы маршрутизации до тех пор, пока снова не станет доступен.

NAT

Сетевая служба NAT выполняет три важных функции:

1. Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 внешний IP-адрес, за которым работают и получают доступ вовне все внутренние IP-адреса.
2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует, они не пропускаются.
3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт для осведомлённых посетителей можно будет попасть по адресу http://zyxel.ru:54055, но на внутреннем сервере, находящимся за NAT, он будет работать на обычном 80-м порту.

Недостатки NAT:

Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов.

Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в протоколах FTP, SIP)

Типы NAT

Тип NAT Virtual Server (port forwarding) (рис. 15) - делает ресурсы в частной сети за ZyWALL доступными для доступа за пределами локальной сети. Публичный IP-адрес подменяется на локальный IP-адрес.

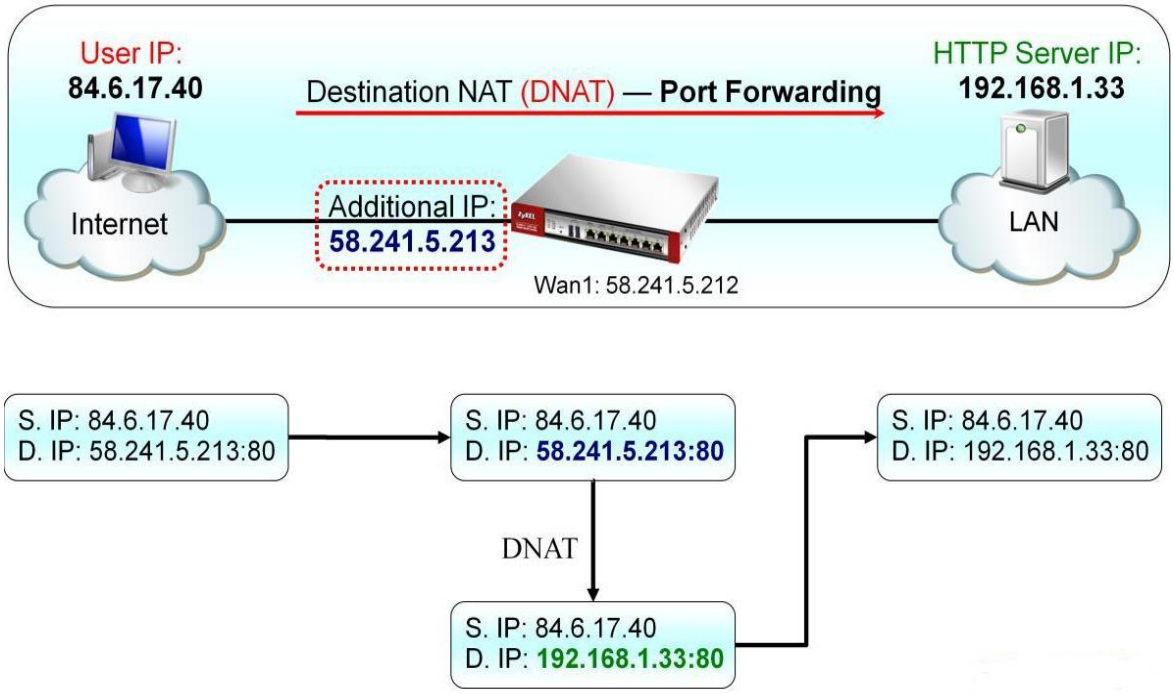


Рис. 15. Virtual Server (port forwarding)

Этот тип NAT не будет выполнять PAT (Port address translation) — все пакеты, полученные на публичный IP-адрес будут просто перенаправлены на локальный IP-адрес.

Virtual Server (port translation) - публичный IP-адрес подменяется на локальный IP-адрес, при этом, опционально, выполняется Port address translation (PAT). Этот тип NAT (рис. 16) выполняет более гибкое сопоставление, которое не только подменяет IP-адрес, но и номер порта.

Для настройки правила Virtual Server в GUI потребуется указать внешний интерфейс, на который будут приходить пакеты.

В роли Original IP указывается IP-адрес, установленный на этом внешнем интерфейсе, или IP-адрес, маршрутизируемый через тот же шлюз по умолчанию.

В роли Mapped IP указывается IP-адрес сервера в локальной сети.

Также нужно указать порты и тип протокола, для которых создается политика. Маршруты создаются системой автоматически.

Для включения функции NAT Loopback (рис. 17) должен быть обязательно указан адрес «Original IP».

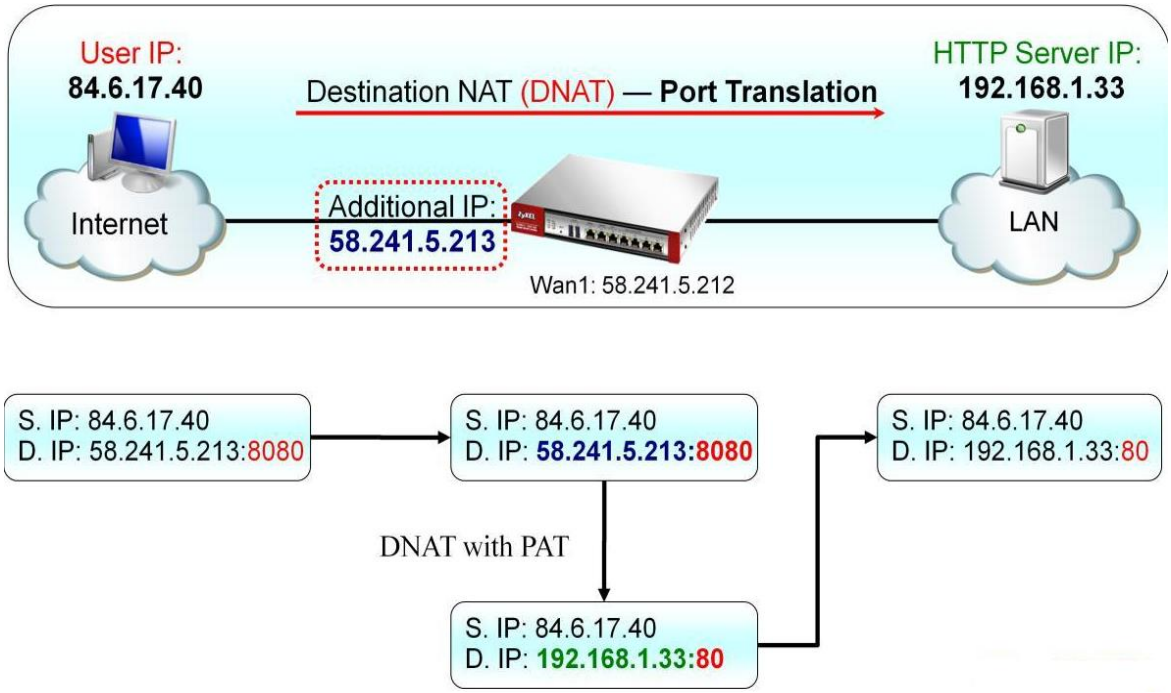


Рис. 16. Virtual Server (port translation)

NAT Loopback

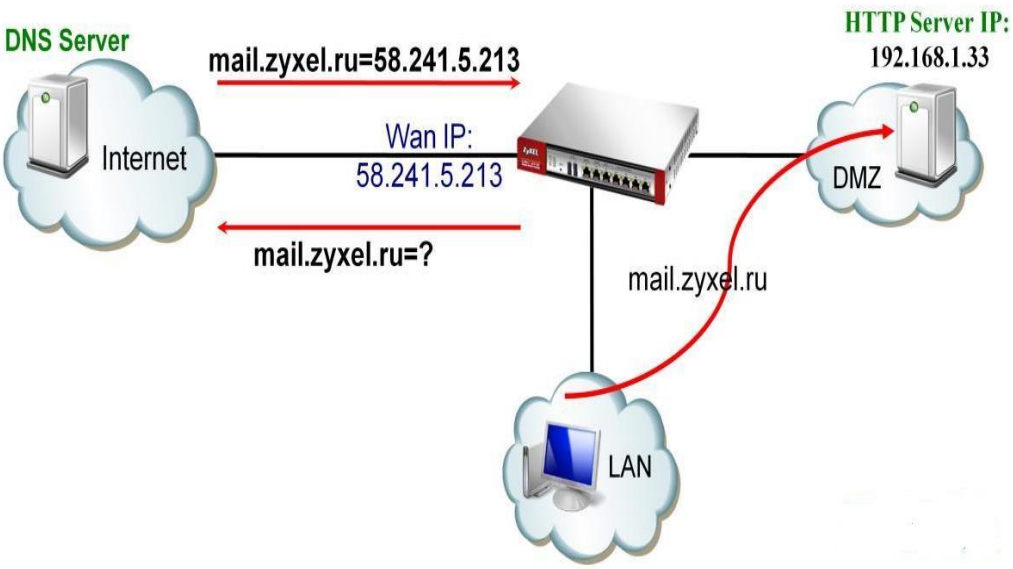


Рис. 17. NAT Loopback

При использовании параметра «any» активировать NAT Loopback нельзя. NAT Loopback – требуется, если настроено правило NAT для передачи трафика из

WAN к серверу в локальной сети, чтобы пользователи, подключенные к другим интерфейсам, также имели доступ к этому серверу.

Контрольные вопросы по теме 1

1. Каковы возможности управления шлюзами?
2. Каковы возможности аутентификации шлюзов?
3. Каковы возможны роли портов?
4. Что такое зоны и каково их назначение?
5. Каково число виртуальных Ethernet интерфейсов?
6. Что такое WAN Trunk и каково его назначение?
7. Каковы алгоритмы балансировки нагрузки?
8. Что такое NAT, типы NAT?

Тема 2. VPN

VPN (Virtual Private Network) – логическая сеть, создаваемая при помощи программных или аппаратных средств поверх другой сети, например, Интернет, при этом способная обеспечить безопасность передаваемых данных.

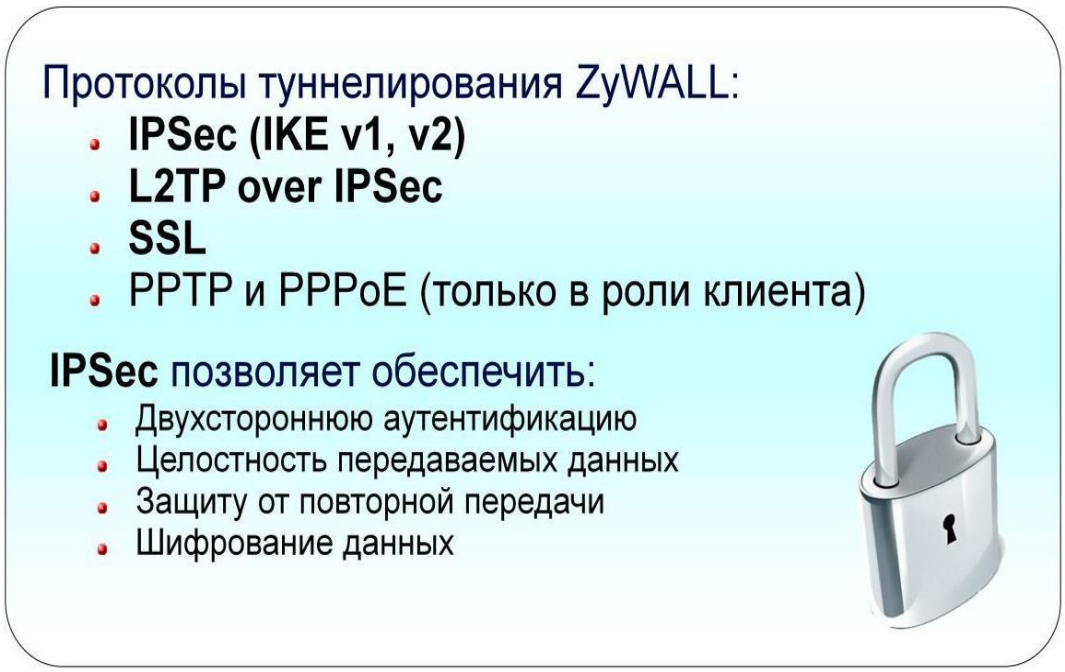


Рис. 18. Протоколы туннелирования

В зависимости от протокола, с помощью которого строится сеть VPN (рис. 18), возможно решить следующие задачи:

1. шифрование данных
2. аутентификация источника
3. проверка целостности данных
4. защита от повторной передачи

Особенности, недостатки и преимущества каждого из протоколов туннелирования – это отдельная и весьма обширная тема. Необходимо отметить, что по ряду причин наиболее распространенным протоколом VPN в

настоящее время является IPSec. Более 65% частных виртуальных сетей созданы на его основе. При помощи набора протоколов IPSec можно реализовать защиту передаваемых данных и аутентификацию на базе следующих услуг.

Шифрование - при использовании IPSec весь передаваемый трафик может быть зашифрован перед передачей по сети.

Целостность - при использовании IPSec получатель может проверить целостность пакетов данных, переданных отправителем, чтобы убедиться в том, что данные не были изменены в процессе передачи.

Аутентификация - при использовании IPSec получатель сообщения может верифицировать источник полученных пакетов и удостовериться в целостности данных

Защита от повторной передачи - необходимо быть уверенным в том, что транзакция может осуществляться только один раз (за исключением случая, когда пользователь уполномочен повторять ее). Это означает, что не должно существовать возможности записи транзакции и последующего ее повторения в записи с целью создания у пользователя впечатления об осуществлении нескольких транзакций. Представим, что мошенник получил информацию о трафике (не взламывая при этом шифра) и знает, что передача такого трафика может дать ему какие-то преимущества (например, в результате на его счет будут переведены деньги). Необходимо обеспечить невозможность повторной передачи такого трафика.

Протоколы IPsec

Протоколы IPsec работают на сетевом уровне (уровень 3 модели OSI). IPsec-протоколы можно разделить на два класса: протоколы, отвечающие за защиту потока передаваемых пакетов, и протоколы согласования ассоциаций защиты.

На настоящий момент определён только один протокол согласования ассоциаций защиты — IKE (Internet Key Exchange), который работает на базе протокола ISAKMP (Internet Security Association and Key Management Protocol), и два протокола, обеспечивающих защиту передаваемого потока:

1. ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных) обеспечивает целостность и конфиденциальность передаваемых данных
2. AH (Authentication Header — аутентифицирующий заголовок) гарантирует только целостность потока (передаваемые данные не шифруются)

SA (Security Associations) — ассоциации защиты, представляют собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон. Составляющими такой политики может быть алгоритм шифрования, алгоритм аутентификации и т.д.

Обзор IPSec

При установлении безопасного туннеля IPsec в первую очередь отрабатывает протокол IKE, который состоит из 2-х стадий.

Стадия 1.

Главной целью обмена данными, происходящего в первой фазе IKE, является аутентификация сторон IPSec и создание защищенного канала между сторонами, позволяющего начать обмен IKE.

Для этого согласовываются SA IKE (алгоритм шифрования, алгоритм аутентификации, секретный ключ).

Стадия 2.

Задачей второй фазы IKE является согласование параметров ассоциации защиты IPSec с целью создания безопасного туннеля IPSec.

Согласовываются следующие параметры: алгоритм шифрования, алгоритм аутентификации, секретный ключ, используемый протокол, используемый режим работы.

Согласование на первой стадии может проходить в одном из двух режимов (Основной или Энергичный), согласование на стадии 2 может проходить только в одном режиме (Быстрый).

После согласования ассоциаций защиты IPSec и создания безопасного туннеля (Стадия 2 IKE) начинают работать протоколы AH или ESP, с помощью которых мы защищаем поток передаваемых данных.

Шифрование данных применяется только при использование протокола ESP.

При использовании протокола AH шифрование данных не применяется, поэтому выбор протокола шифрования отсутствует.

При необходимости можно рассчитать ключ повторно или взять из первой стадии.

IPsec VPN. AH/ESP. Tunnel/Transport mode

Существует две типа протоколов IPsec, обеспечивающих защиту потока передаваемых пакетов: ESP (Encapsulation Security Payload, инкапсуляция зашифрованных данных) и AH (Authentication Header, Аутентифицирующий заголовок). ESP и AH - новые протоколы IP.

О том, что пакет является пакетом ESP, говорит значение в поле протокола заголовка IP, равное 50, а для пакета AH - равное 51.

Рис. 19 демонстрирует исходный пакет IP и пакеты IP при передаче по протоколам ESP и AH соответственно.

В пакетах ESP и AH между заголовком IP (IP header) и данными протокола верхнего уровня вставляется заголовок ESP/AH (ESP/AH header).

ESP может обеспечивать как шифрование, так и аутентификацию, а также возможен вариант протокола ESP без шифрования.

При осуществлении шифрования заголовок ESP не шифруется, но шифруются данные протокола верхнего уровня и часть трейлера ESP.

А в случае аутентификации производится аутентификация заголовка ESP, данных протокола верхнего уровня и части трейлера ESP.

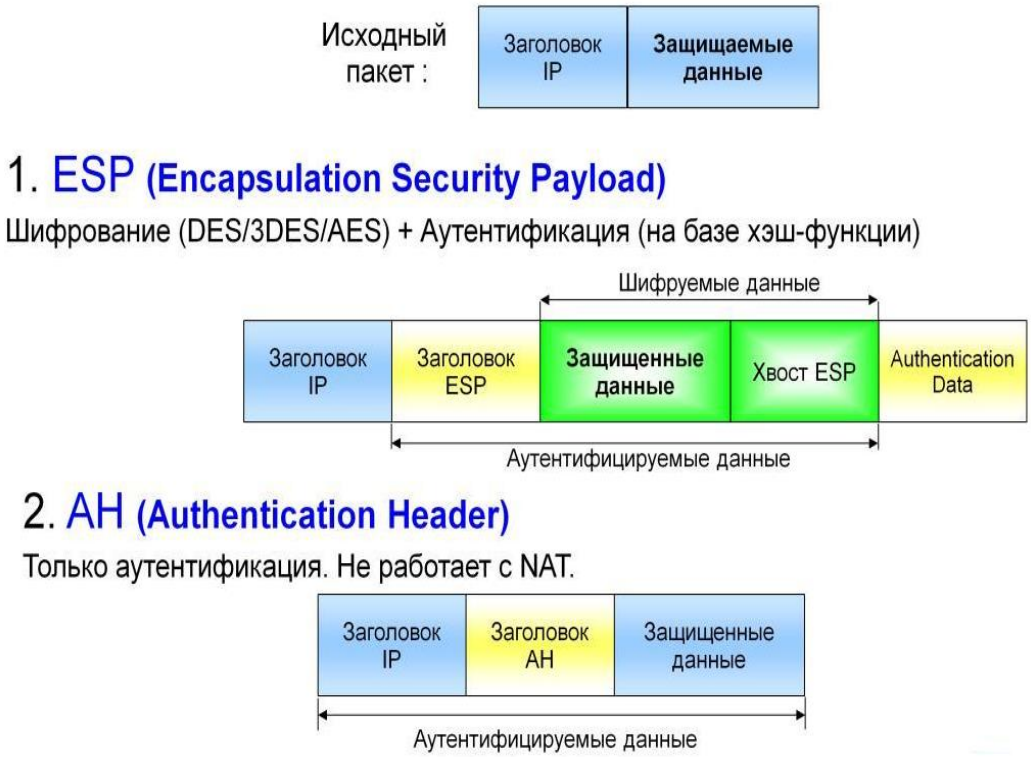


Рис. 19. Протоколы защиты

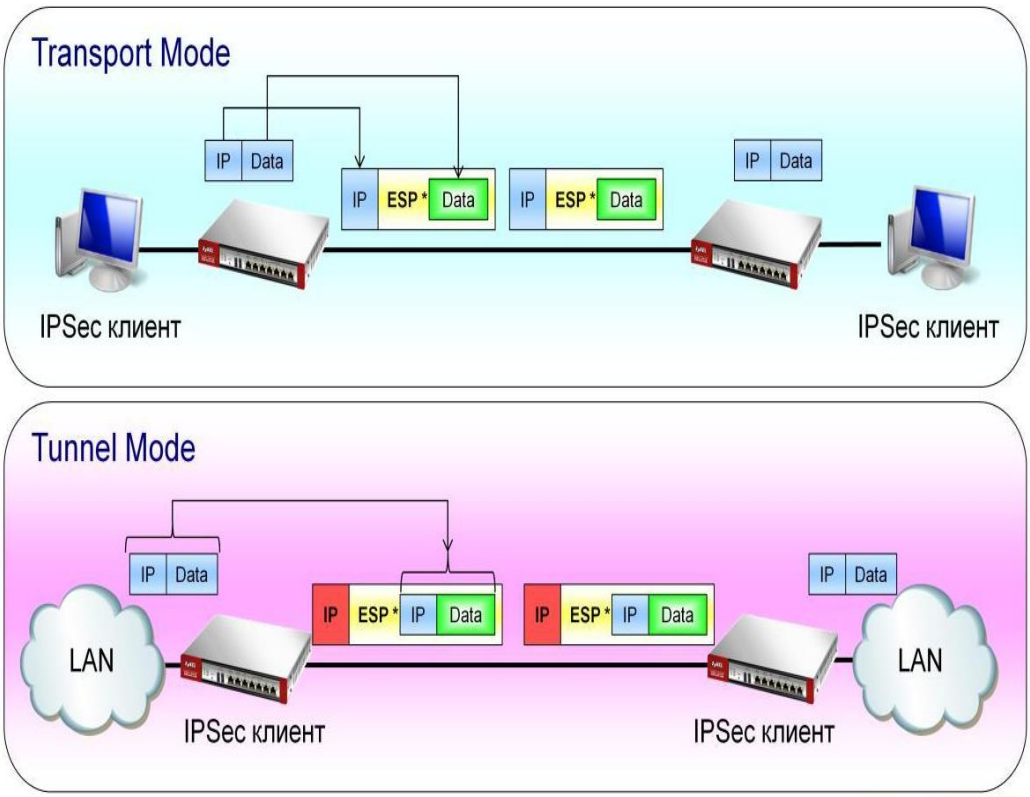


Рис. 20. Transport / Tunnel Mode

Хотя протокол AH может обеспечивать только аутентификацию, она выполняется не только для заголовка AH и данных протокола верхнего уровня, но также и для заголовка IP.
AH и ESP также позволяют обеспечить целостность данных и защиту от повторной передачи.
Протокол AH и протокол ESP могут работать в двух режимах, в транспортном и в туннельном (рис. 20).

Транспортный режим

Транспортный режим обеспечивает безопасное соединение двух узлов путем инкапсуляции тела IP-пакета в пакет AH либо ESP.
Таким образом, клиент IPsec и источник/получатель данных – это одно устройство, то есть соединение точка-точка.

Туннельный режим

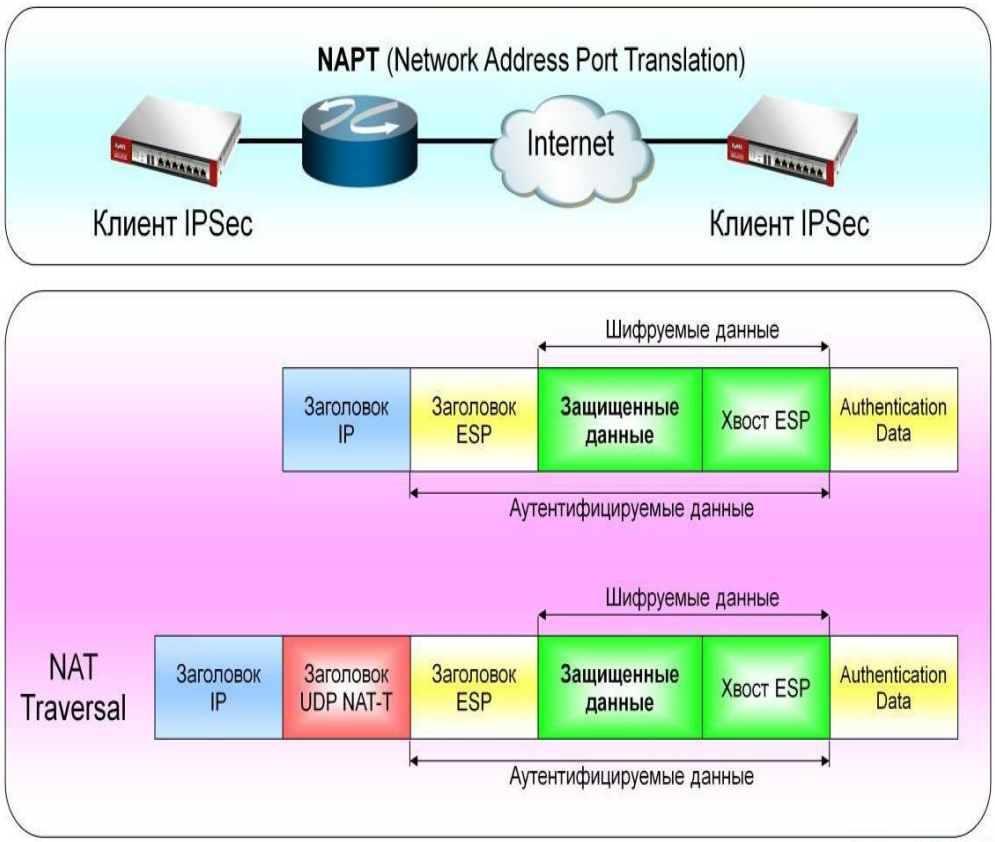


Рис. 21. NAT Traversal

Туннельный режим инкапсулирует весь IP-пакет в пакет AH либо ESP.
Таким образом, клиентом IPsec и источником/получателем данных могут быть разные устройства. Чаще всего используется именно туннельный режим.
Аналогичный процесс происходит при использовании протокола AH, за исключением того, что в AH данные не шифруются.
В случае если в сети между шлюзами безопасности присутствует (рис. 21) NAT, то:

1. протокол AH работать **не** будет
2. протокол ESP работать будет

В случае если в сети между шлюзами безопасности присутствует реализация NAPT (Network Address Port Translation):

1. протокол AH работать не будет
2. протокол ESP работать не будет

Функция NAT Traversal (NAT-T) позволяет обеспечить работоспособность протокола ESP в случае, если между шлюзами безопасности присутствует NAPT (network address port translation).
Однако NAT-T не позволяет обеспечить работоспособность протокола AH. Данная функция описана в RFC 3947 и RFC 3948.
Принцип работы функции NAT-T заключается в том, что между IP заголовком и ESP заголовком дополнительно помещается UDP заголовок.

Режим VPN — Site-to-Site

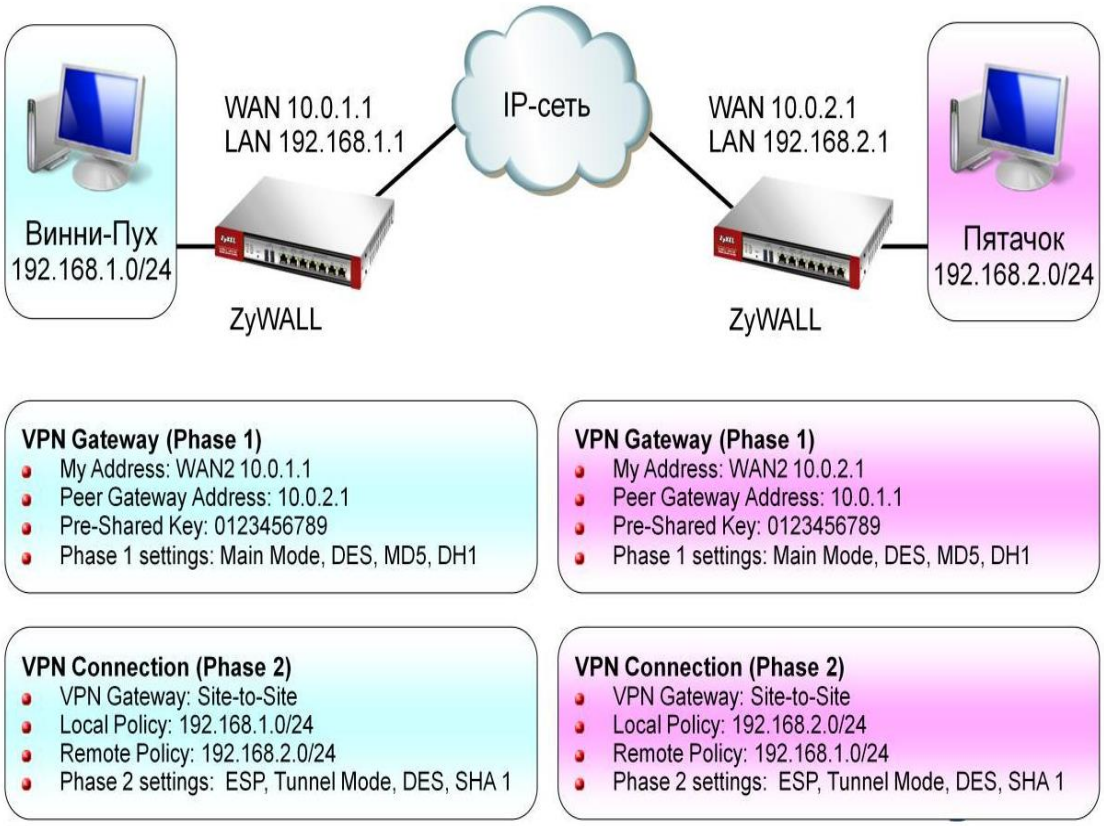


Рис. 22. Site-to-Site IPsec VPN

Наиболее часто используемый режим VPN — Site-to-Site, это схема, в которой безопасное соединение организуется между двумя сетями.
Для того, чтобы создать Site-to-Site VPN, необходимо на обеих сторонах туннеля настроить параметры первой и второй фазы.
В первой стадии Site-to-Site VPN (рис. 22) необходимо на обеих сторонах туннеля настроить IP-адрес удаленной стороны.
В случае если на удаленной стороне IPадресов несколько на разных интерфейсах, то второй можно указать в поле Secondary.
В таком случае на ZyWALL или USG, с которым будет устанавливаться соединение, нужно будет в поле My Address указать значение 0.0.0.0, для того

чтобы устройство могло установить туннель как с одного, так и с другого интерфейса.

Во второй стадии Site-to-Site VPN, необходимо указать значение локальной подсети и подсети на противоположной стороне устанавливаемого туннеля.

IPsec VPN. Site-to-Site with Dynamic Peer

Для случая, когда удаленная сторона имеет динамический адрес, на рис. 23 показаны необходимые настройки.

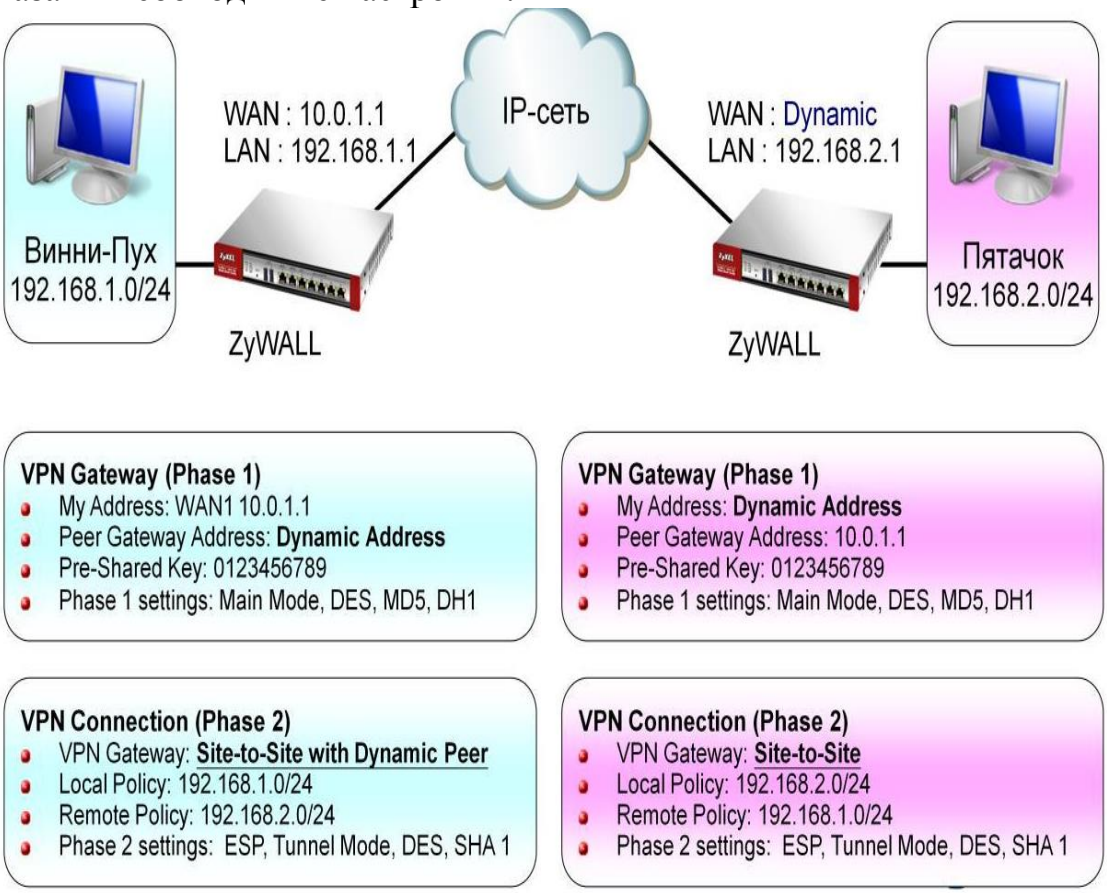


Рис. 23. Динамический адрес с одной стороны

Site-to-Site with Dynamic Peer очень похож на Site-to-site VPN, отличие заключается только в том, что удаленная сторона имеет динамический IP-адрес. Такой тип VPN туннеля может быть установлен только со стороны, которая имеет динамический IP-адрес.

В случае, если на обеих сторонах IPsec VPN туннеля используются динамические (рис. 24) IP-адреса, необходимо использование дополнительной функции DynDNS.

Дополнительная функция DynDNS позволяет сопоставить постоянное доменное имя динамическому IP адресу.

Далее при настройке IPsec VPN в качестве адреса удаленного шлюза будет использоваться постоянное доменное имя.

Например, используется сервис DtDNS:

1. Заполнить имя пользователя и пароль для входа в учетную запись DDNS.

2. Заполнить имя домена. В примере – zytestusgdr.dtdns.net
3. Привязать к требуемому внешнему интерфейсу. В примере – PPPoE на WAN 1 интерфейсе
4. Указать сервер DYNDNS: www.dtdns.com
5. Указать ссылку, предоставленную сервисом URL: /api/autodns.cfm?id=**value**&pw=**value nETW**

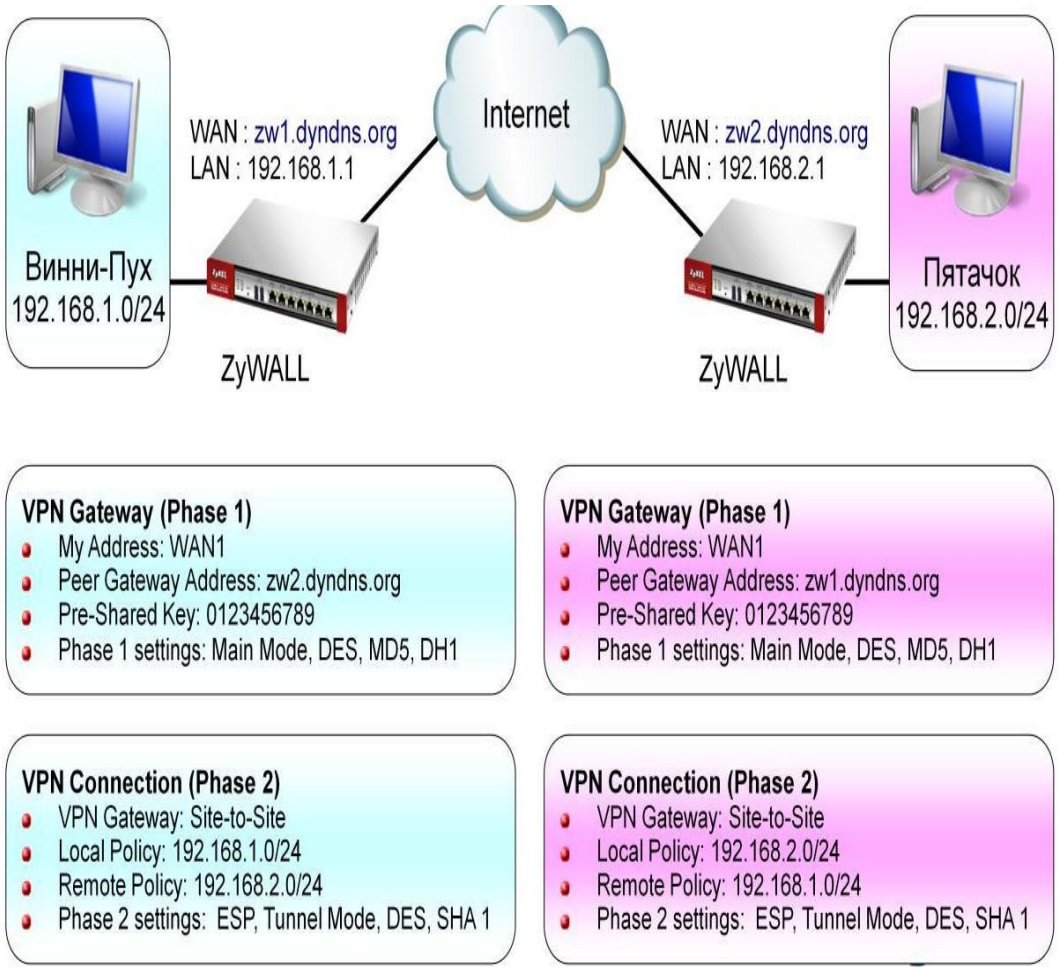


Рис. 24. Динамический адрес с двух сторон

Настройка распложена в меню CONFIGURATION> Network> DDNS

IPsec VPN Использование сертификатов

Устройства ZyWALL и USG могут использовать цифровые сертификаты для аутентификации.

Первое, что необходимо сделать - это добавить подписанный сертификат того узла, которому доверяют в Trusted Certificates.

Необходимо сгенерировать и подписать свой сертификат в My Certificates, загрузить его в доверенные на удаленной стороне.

Существует довольно большое число компаний, которые предоставляют платный сервис создания и подписи цифровых сертификатов.

Так же можно сделать самоподписанный сертификат.

ZyWALL и USG поддерживает следующие форматы сертификатов для добавления:

1. Binary X.509
2. PEM (Base-64) encoded X.509
3. Binary PKCS#7
4. PEM (Base-64) encoded PKCS#7
5. Binary PKCS#12

Создание сертификата

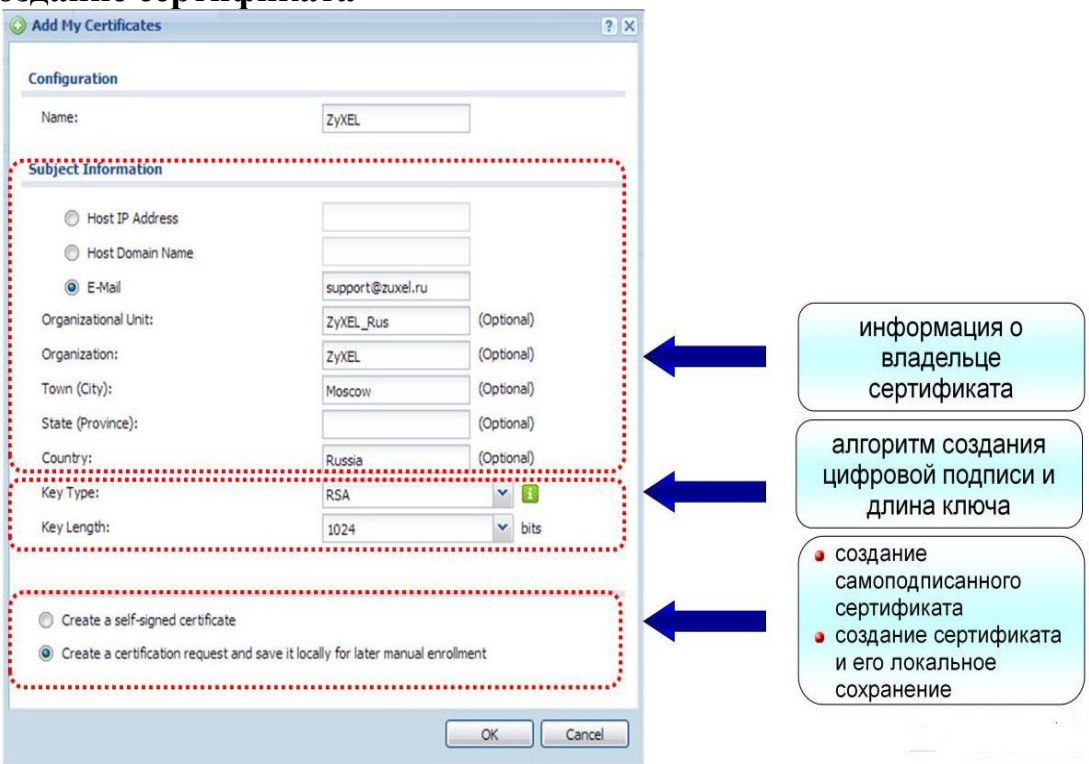


Рис. 25. Создание сертификата

При создании сертификата (рис. 25) возможны следующие варианты:

1. создание самоподписанного сертификата, то есть ZyWALL в данном случае будет выступать в качестве центра сертификации, и именно к нему будут обращаться для проверки его же сертификата, данный метод не рекомендуется применять по причине низкой надежности
2. создание сертификата и локальное сохранение его с последующей ручной отправкой в центр сертификации на подпись

При создании сертификата по возможности выбирается максимальная длина ключа, тем самым увеличивается его криптостойкость.

Пример использования сертификатов на устройствах ZyWALL или USG — для аутентификации при создании IPsec VPN туннеля.

Также сертификаты можно применять для аутентификации при создании SSL VPN туннеля и в других функциях, использующих сертификаты.

IPsec VPN. IKEv2

Наряду с IKEv1 (RFC 2407, 2408, 2409, 4109, 4995) в шлюзах безопасности ZyWALL и USG реализована поддержка протокола IKEv2 (RFC5996) с аутентификацией EAP.

По сравнению с IKEv1, протокол IKEv2 обеспечивает более быстрое и безопасное согласование ассоциаций безопасности IKE SA/IPsec SA, генерацию ключей шифрования безопасности и лучшую защиту от DoS-атак.

Кроме того, IKEv2 и EAP штатно поддерживаются операционными системами Windows 7/8, что позволяет использовать эти технологии для организации удаленных рабочих мест для выездных сотрудников без необходимости устанавливать на компьютере сотрудника дополнительное программное обеспечение.

А встроенные DPD и NAT-T в протокол позволят повысить стабильность туннелей и передаваемых в них данных.

Настройка IKEv2 Phase 1

Настройка IKEv2 Phase 1 имеет следующие особенности.

1. IKE v2 несовместим с IKE v1
2. Поддерживается только аутентификация EAP MS-CHAPv2
3. Встроенный клиент Windows VPN не поддерживает раздельного туннелирования (split tunnel)
4. В существующем правиле «Фазы 1» нельзя изменить версию IKE. Нужно добавить новое правило вместо изменения текущего правила.

Настройка IKEv2 Phase 2

В настройках правила для клиента Windows 7/8 потребуется использовать следующее сочетание протоколов шифрования и аутентификации:

Фаза 1:

3DES-SHA1-DH2

AES128-MD5-DH2

AES128-SHA1-DH2

Фаза 2:

3DES-SHA1

AES128-SHA256

AES256-SHA1

Сертификат ZyWALL, используемый для построения туннеля, нужно загрузить в «Доверенные корневые центры сертификации».

Настройки клиента Windows 7/8 выглядят следующим образом:

1. Type of VPN: IKEv2
2. Data encryption: Require encryption (disconnect if server declines)
3. Authentication: Use MSCHAP v2

Также потребуется загрузить используемый для туннеля сертификат с ZyWALL и добавить его в доверенные сертификаты на ПК клиента.

L2TP VPN over IPsec

Технология L2TP VPN over IPsec (рис. 26) реализована в большинстве современных мобильных устройств, таких как, например, устройства с операционной системой Android или IOS, которая обеспечивает пользователям безопасный удаленный доступ к ресурсам корпоративной сети со своих смартфонов или планшетных компьютеров.
Настройка L2TP over IPsec производится в меню Quick Setup шлюза.
Настройка подключения L2TP over IPsec возможна и с обычного настольного компьютера.
В микропрограммах алгоритм шифрования 3DES, необходимый для создания VPN-туннеля с ОС Windows 7/Vista, iPhone (iOS), смартфонами (Android), доступен только при выполнении следующих инструкций:

1. Микропрограммы для аппаратных шлюзов серии ZyWALL и USG, представленные на сайте в разделе Центр загрузки, позволяют использовать только шифрование DES для туннелей IPsec VPN и SSL VPN. Это ограничение вызвано тем, что шифровальные средства с криптографическим ключом более 56 бит запрещены для использования на территории Таможенного союза России, Белоруссии и Казахстана.
2. Данное ограничение применяется на всех устройствах серий ZyWALL и USG с кодом страны e6 (Россия).
3. Отключить ограничения, накладываемые кодом страны, можно с помощью следующих команд:

   Router> **configure terminal**

   Router(config)# **crypto algorithm-hide disable**

   Router(config)# **write**

   Router(config)# **reboot**

Файлы конфигураций устройства модифицируются, поэтому их необходимо сохранять перед обновлением микропрограммы.
Последним шагом потребуется проверить параметры, которые будут выдаваться пользователю после того, как туннель будет установлен. Также дополнительно потребуется создать правила маршрутизации и политики межсетевого экрана, в зависимости от того, куда должен будет маршрутизироваться трафик от пользователей.
Максимальное количество одновременно установленных туннелей зависит от того, какая модель ZyWALL или USG используется, и будет равно количеству IPsec VPN в устройстве.
Во многих операционных системах L2TP VPN over IPsec туннель имеется по умолчанию и прост в настройке.

При использовании L2TP VPN over IPsec туннелей совместно с ZyWALL или USG не потребуется дополнительных лицензий.

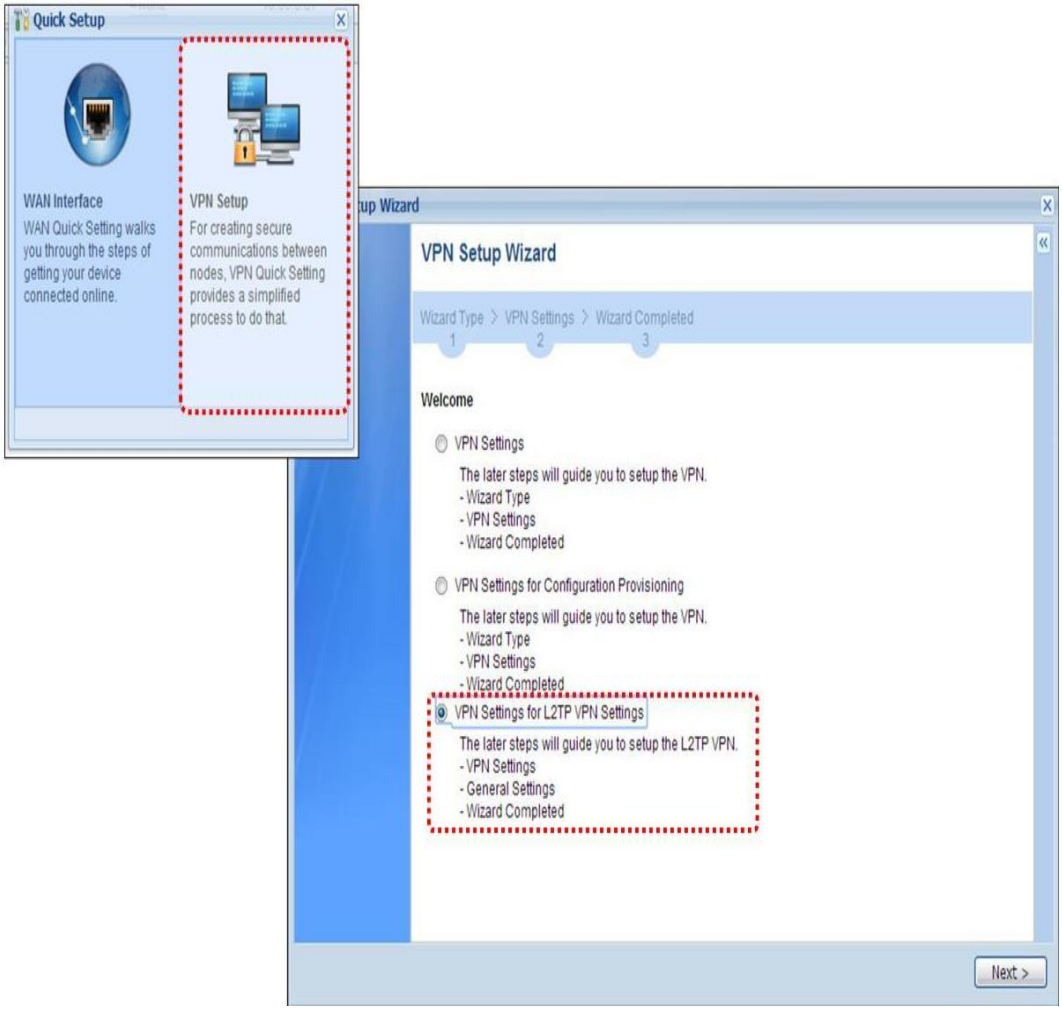


Рис. 26. Быстрая настройка L2TP over IPsec VPN

Туннелей L2TP VPN over IPsec можно установить столько, сколько позволяет конкретная модель ZyWALL или USG установить IPsec туннелей.

SSL VPN

SSL VPN — это механизм обеспечения безопасных каналов связи, то есть аутентификации, шифрования, целостности данных от удаленного пользователя до шлюза безопасности, используя протокол SSL (Secure Sockets Layer).

Данная функция применяется как альтернатива IPSec VPN для удаленных пользователей, так как SSL VPN не требует дополнительного программного обеспечения IPSec VPN клиента, достаточно браузера с поддержкой SSL и не требует дополнительного оборудования (аппаратного IPSec VPN клиента).

SSL VPN на ZyWALL и USG может работать в двух режимах.

Reverse Proxy Mode

В режиме Reverse Proxy ZyWALL для удаленного клиента выступает в роли прокси сервера и обеспечивает доступ к любым веб-приложениям и общим

файлам и папкам. Режим Reverse Proxy не требует установки дополнительного программного обеспечения, достаточно иметь браузер.

Full Tunnel Mode

В режиме Full Tunnel создается виртуальное соединение между удаленным клиентом и ZyWALL, удаленный клиент получает ip-адрес из указанной вами сети, что позволяет ему использовать любые ресурсы локальной сети так же, как если бы он физически находился в локальной сети.

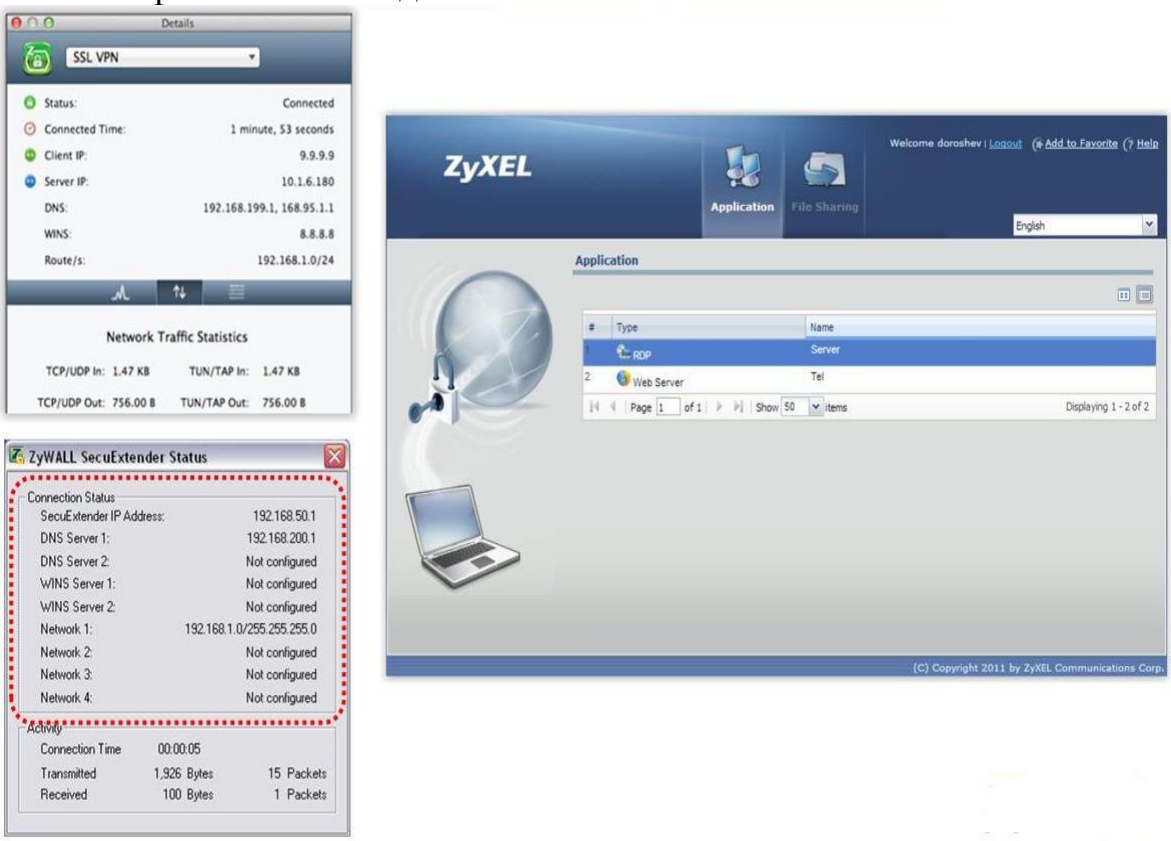


Рис. 27. Использование SSL

В режиме Reverse Proxy удаленному клиенту доступны 2 типа сервисов:

- **Web-Application**

Web Server – доступ к web-сайту, расположенному внутри локальной сети. OWA (Outlook Web Access) – доступ к e-mails, contacts, calendars с помощью Microsoft Outlook-like interface в веб-браузере.

VNC – доступ к Virtual Network Computing remote desktop server.

RDP – Remote Desktop Protocol remote desktop server. Weblink – ссылка на веб-страницу.

- **File Sharing**

Access Policy — политика, которая определяет, какой удаленный пользователь к каким ресурсам внутренней сети может иметь доступ.

В случае использования Reverse Proxy Mode необходимо:

1. выбрать пользователей/группу пользователей, к которым будет применяться данная политика

2. выбрать сервисы, которые будут доступны данным пользователям

Раздел настройки Network Extension не заполняется, он используется для реализации Full Tunnel Mode.

Для установления безопасного соединения между удаленным пользователем и ресурсами локальной сети пользователь должен зайти на веб-интерфейс ZyWALL USG, ввести свой логин и пароль и нажать кнопку SSL VPN.

После успешной аутентификации удаленный пользователь увидит веб-приложение, котором ему будут доступны два типа сервисов:

1. Application
2. File Sharing

SSL VPN. Full Tunnel Mode

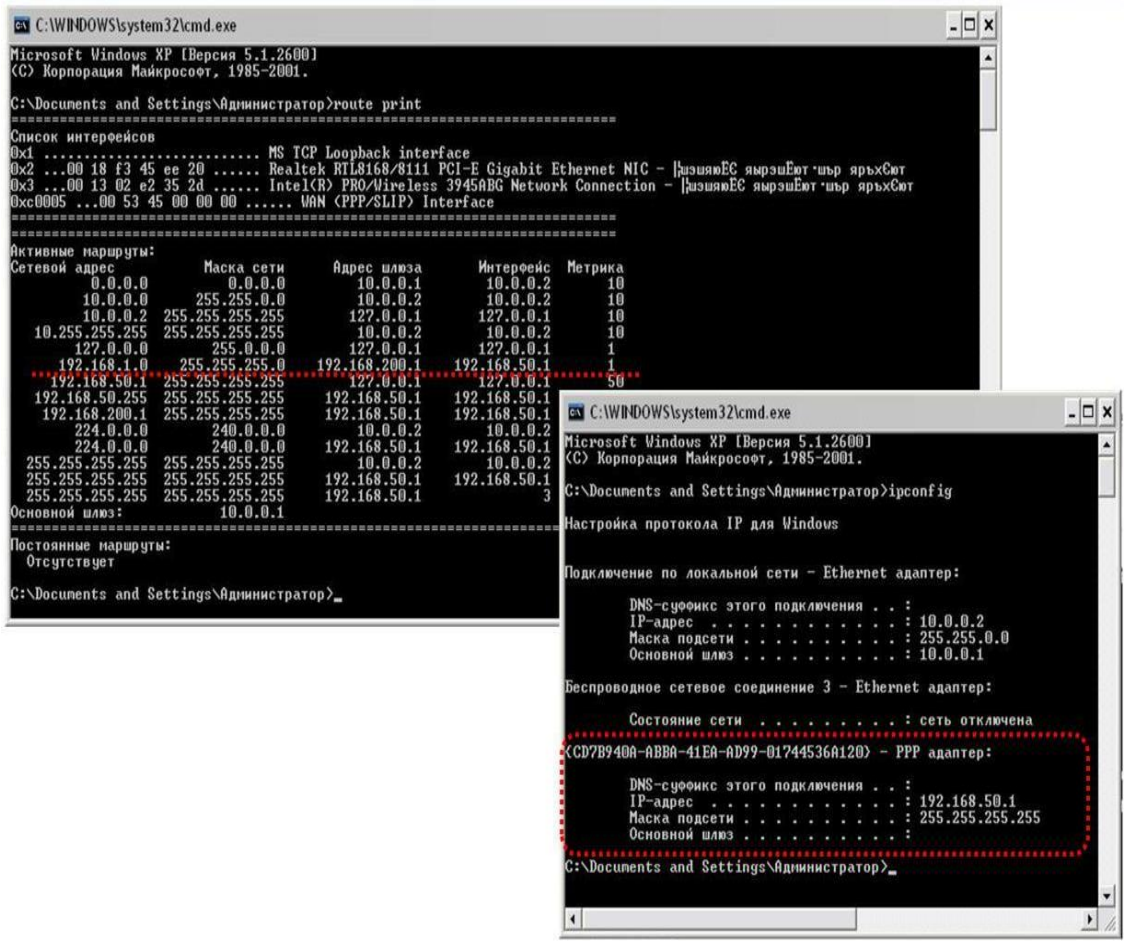


Рис. 28. Использование SSL (2/2)

В случае использования Full Tunnel Mode необходимо выполнить:

1. выбрать пользователей/группу пользователей, к которым будет применяться данная политика
2. выбрать сервисы, которые будут доступны данным пользователям
3. задать дополнительные настройки Network Extension, а именно:
4. диапазон IP-адресов, из которого будут выдаваться адреса клиентам на виртуальные соединения

5. адреса DNS и WINS серверов
6. список хостов/подсетей к которым удаленный пользователь будет иметь доступ через виртуальное соединение

В случае успешной аутентификации удаленного пользователя на стороне ZyWALL, пользователь увидит (рис. 27) информацию об установившемся виртуальном соединении, в котором показаны следующие параметры:

1. IP-адрес пользователя на виртуальном соединение
2. адреса DNS и WINS серверов
3. список сетей/хостов к которым пользователь получил доступ

Состояние текущих SSL VPN сессий можно посмотреть в соответствующем меню, любую текущую SSL VPN сессию можно принудительно разорвать.

После установки приложения для работы SSL-туннеля в режиме Full Tunnel, добавляется (рис. 28) дополнительный PPP адаптер на ПК клиента.

Когда туннель будет установлен, на данный PPP адаптер автоматически будет получен IP-адрес из пула адресов, которые были выделены на ZyWALL.

Так же в политиках маршрутизации будут добавлены новые маршруты к тем сетям, к которым пользователь имеет доступ.

Контрольные вопросы

1. Каково назначение VPN?
2. Назвать протоколы IPsec.
3. Что такое Site-to-Site и его назначение?
4. Что такое Site-to-Site with Dynamic Peer?
5. Назначение и использование сертификатов.
6. Каково назначение IKE v2?
7. Что такое Virtual Server (port forwarding)?
8. Что такое Tunnel и Transport mode?
9. Каково назначение L2TP VPN over IPsec?
10. Каково назначение SSL VPN?

Тема 3. Unifies security policy

Концепция унифицированных политик безопасности (Unified Security Policy), совмещает в себе правила межсетевого экрана с профилями сервисов безопасности, такими как антивирус, защита от вторжений, управление сетевыми приложениями, контентная фильтрация, антиспам и инспекция SSL. В рамках этой концепции к каждому правилу межсетевого экрана можно привязать нужные, предварительно настроенные профили упомянутых сервисов.

Unified Security Policy делает процесс конфигурирования устройства ZyWALL более простым и логичным, а также добавляет чрезвычайную гибкость в применении сервисов безопасности.

Политики безопасности

Пользователи могут применять политики межсетевого экрана и различных функции UTM с помощью единого интерфейса.

Привязывать на различные направления профили UTM, тем самым контролировать передаваемые данные на уровнях 3-7 модели OSI.

Настройка в три шага представляет собой:

1. Создание объекта: приложения, типа трафика, запроса и т.д.
2. Создание профиля UTM и использовании в нем ранее созданного объекта
3. Настройка политики безопасности и привязки ранее созданных профилей UTM.

За счет данного механизма достигается максимальная наглядность того, какие правила и политики применяют для тех или иных пользователей.

В зависимости от функции UTM и её назначения созданный профиль может быть привязан к различным Security профилям как для входящего, так и для исходящего направления трафика.

Рассмотрим архитектуру передачи и проверки трафика ZyWALL и USG в упрощенном виде.

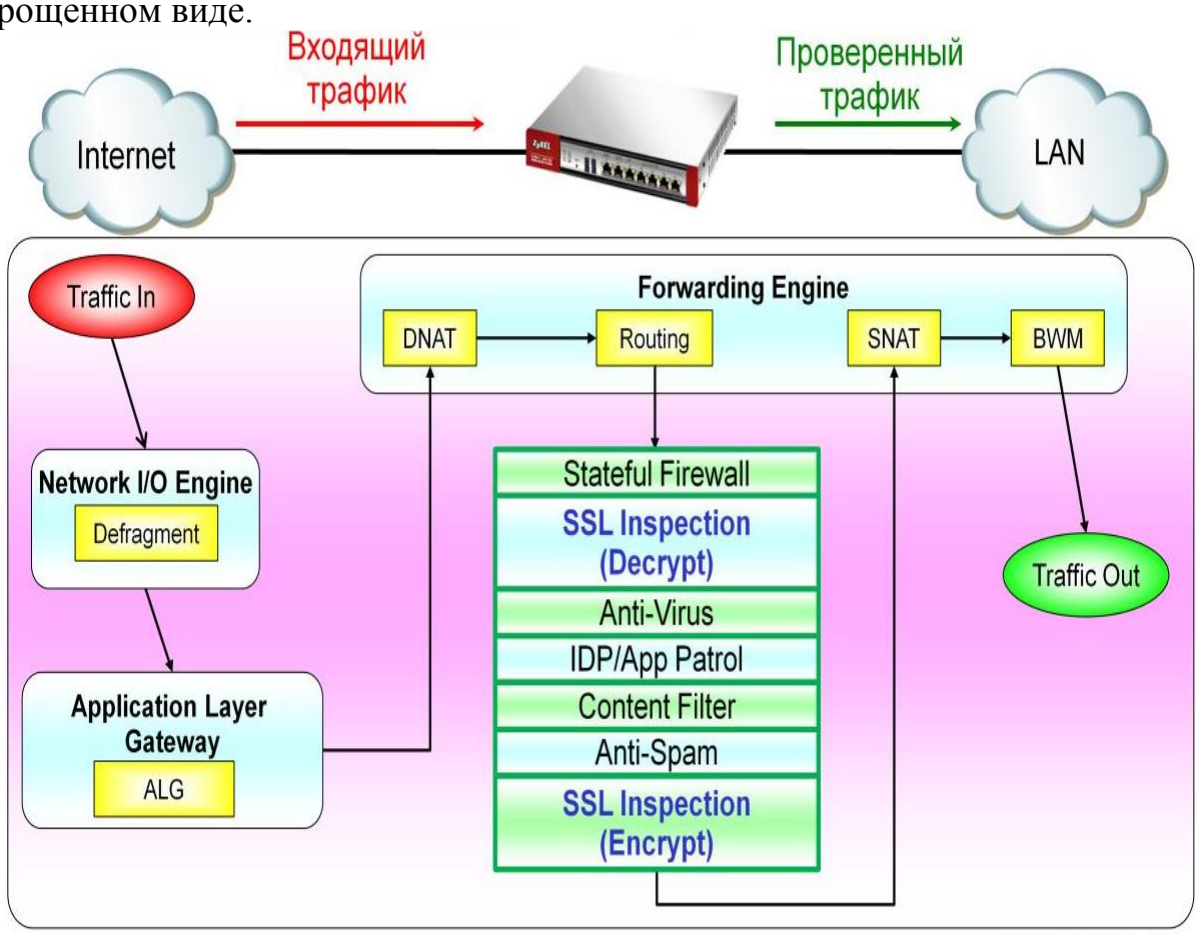


Рис. 29. Порядок пересылки и проверки

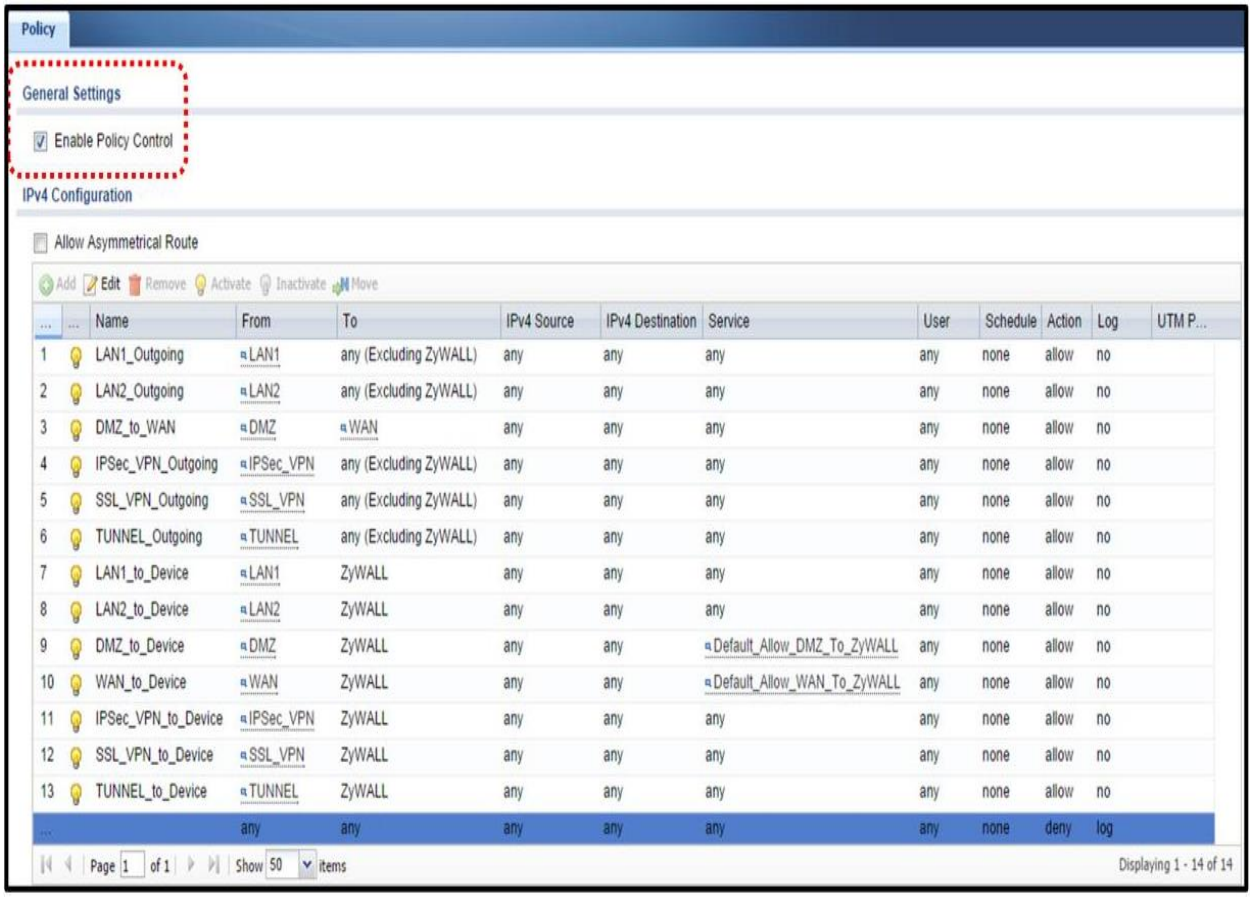
При прохождении трафика через ZyWALL или USG он проходит через несколько (рис. 29) этапов. На первом этапе входящий трафик попадает в буфер обмена, после чего, на втором этапе, к нему может применяться функция ALG

(Application Layer Gateway), позволяющая SIP, H.323 или FTP нормально работать с NAT.
Следующий этап, называющийся Forwarding Engine, состоит из NAT, маршрутизации, анализа и проверки трафика, ограничения пропускной способности.
В устройствах ZyWALL USG понятие NAT разделено на две составляющие: DNAT — в случае если передача трафика была инициирована из внешней сети по публичному IP-адресу, и SNAT — когда сессия для входящего трафика была установлена из внутренней сети.

Виды Firewall

Пакетные фильтры — фильтры, которые проверяют пакет на сетевом уровне и являются независимыми от приложения. Это позволяет им показывать высокую производительность и масштабируемость. Однако это вид firewall, обеспечивающий наименьшую защиту. Причина в том, что у пакетного фильтра нет информации о приложениях более высокого уровня и нет возможности отслеживать контекст данного соединения. Это делает их уязвимыми для хакеров.
Шлюзы уровня приложения обеспечивают больший уровень безопасности, проверяя все прикладные уровни пакета. При принятии решения используют информацию о текущем контексте. Однако, делая это, они нарушают модель клиент-сервер. Каждое соединение клиент-сервер требует двух соединений: одно от клиента к firewall и другое от firewall к клиенту.
Технология stateful inspection решает проблемы двух предыдущих подходов, обеспечивая полный контроль на уровне приложения без нарушения модели клиент-сервер.
В случае stateful inspection пакет перехватывается на сетевом уровне, после чего ZyWALL извлекает информацию о контексте, необходимую для принятия решения, со всех уровней и сохраняет эту информацию в динамических таблицах для проверки последующих пакетов.
Это обеспечивает решение с высоким уровнем безопасности, дающее максимальную производительность, масштабируемость и расширяемость.
Пример работы stateful inspection:
Механизм stateful inspection отслеживает сессию FTP, поверяя данные на уровне приложения (FTP).
Когда клиент запрашивает сервер об открытии обратного соединения (команда FTP PORT), ZyWALL извлекает номер порта из этого запроса.
В списке запоминаются адреса клиента и сервера, номера портов.
При фиксировании попытки установить соединение FTP-data, ZyWALL просматривает список и проверяет, действительно ли данное соединение является ответом на допустимый запрос клиента.
Список соединений поддерживается динамически, так что открыты только необходимые порты FTP. Как только сессия закрывается, порты блокируются, обеспечивая высокий уровень защищенности.

При настройке Firewall (рис. 30) необходимо указать политики, согласно которым трафик будет отбрасываться или пропускаться.
В случае, если пакет попадает под действие двух или более политик, то он будет обрабатываться той политикой, которая имеет меньший приоритет, то есть находиться выше остальных в списке политик.



		Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log	UTM P...
1		LAN1_Outgoing	LAN1	any (Excluding ZyWALL)	any	any	any	any	none	allow	no	
2		LAN2_Outgoing	LAN2	any (Excluding ZyWALL)	any	any	any	any	none	allow	no	
3		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	
4		IPSec_VPN_Outgoing	IPSec_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no	
5		SSL_VPN_Outgoing	SSL_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no	
6		TUNNEL_Outgoing	TUNNEL	any (Excluding ZyWALL)	any	any	any	any	none	allow	no	
7		LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	allow	no	
8		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no	
9		DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_DMZ_To_ZyWALL	any	none	allow	no	
10		WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_WAN_To_ZyWALL	any	none	allow	no	
11		IPSec_VPN_to_Device	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
12		SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
13		TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
...			any	any	any	any	any	any	none	deny	log	

Рис. 30. Политики Firewall

Последнее правило блокирует пакеты, не разрешенные для передачи остальными правилами.
В качестве критериев, по которым будет определяться, к каким пакетам применять данную политику, можно использовать:

1. **From** — зона источника пакета
2. **To** — зона получателя пакета
3. **Schedule** — расписание работы данной политики
4. **User** — пользователь/группа пользователей, на которых данная политика будет распространяться
5. **Source** — адрес/диапазон адресов/подсеть источника пакета
6. **Destination** — адрес/диапазон адресов/подсеть получателя пакета
7. **Service** — служба, пакеты который будут обрабатываться данной политикой, в качестве критериев можно использовать номера

TCP/UDP портов, типы ICMP ответов, номер протокола в поле Protocol заголовка IP

8. **Access** — действие, которое будет произведено с пакетом, удовлетворяющим всем критериям, возможные варианты: allow, deny, reject
9. **Log** — позволяет заносить записи в Log, в случае если данная политика сработала

ADP (Anomaly Detection and Prevention)

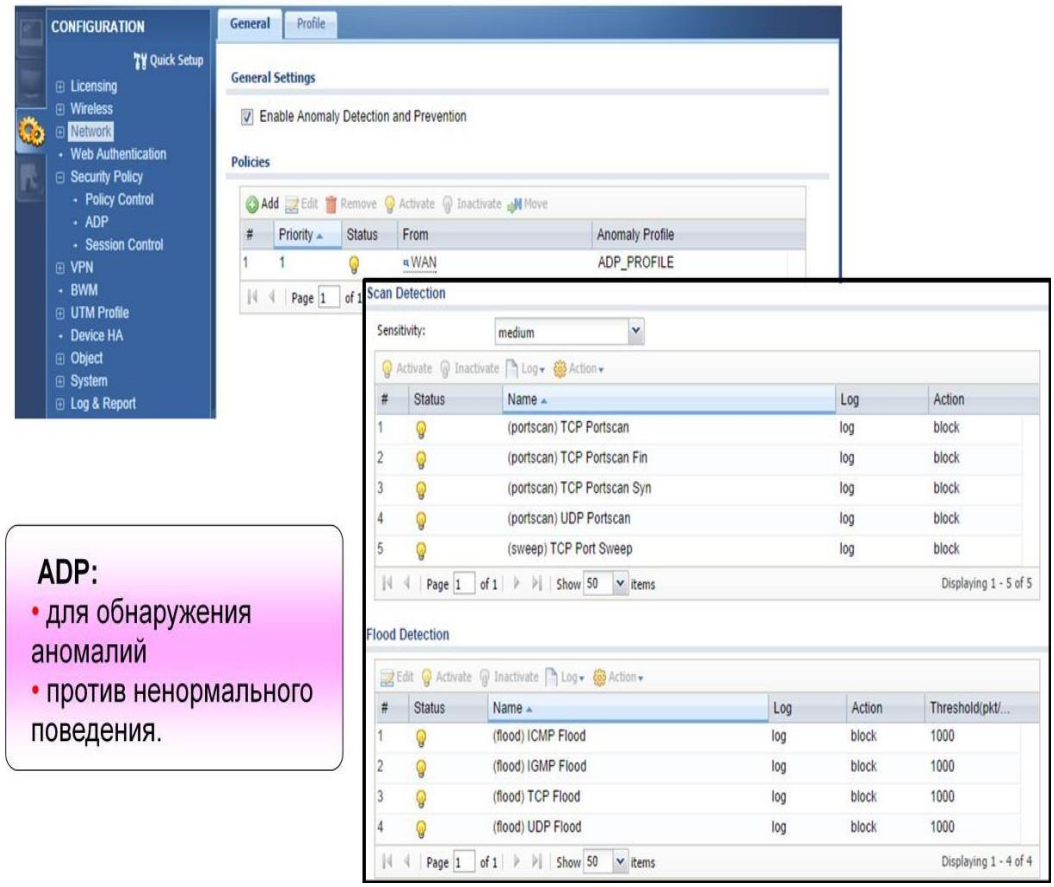


Рис. 31. ADP (Anomaly Detection and Prevention)

Функция шлюзов безопасности ADP защищает от аномалий на основе обнаружения нарушения стандартов протоколов (RFC) и аномальных пакетов, таких как сканирование портов (рис. 31).

Отличия ADP от IDP

1. ADP предназначен для обнаружения аномалий и эффективен против ненормального поведения, а IDP предназначен для проверки пакетов и служит для предотвращения известных атак.
2. ADP политики и правила обновляются, когда загружается новая прошивка в отличие от IDP Packet Inspection, для обновления которой требуется подписка.

IDP (Intrusion Detection &Protection)

IDP (система обнаружения и предотвращения вторжений) — это функция, в задачи которой входит обнаружение и защита сети от попыток взлома и прочих «хакерских» деяний.

Принцип работы функции IDP основывается на поиске известных сигнатур в проходящих пакетах, аналогично работе функции антивируса (рис. 33).

Процесс настройки функции IDP заключается в создании профилей (политик) и последующем назначении профилей на любые направления передачи трафика.

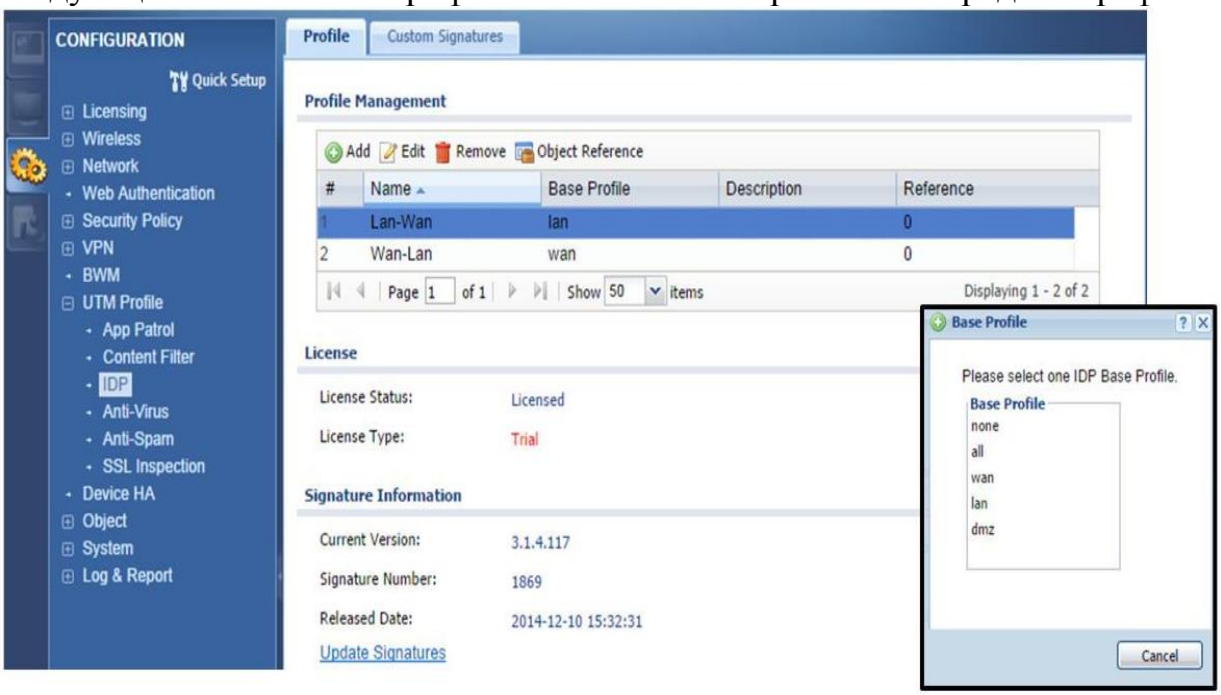


Рис. 33. IDP (Intrusion Detection & Protection)

Профиль IDP (рис. 34) содержит список известных сигнатур, а также информацию о том, будет ли ZyWALL искать данную сигнатуру в потоке пакетов и какое действие будет произведено в случае нахождения.

Возможны следующие действия в случае нахождения сигнатуры:

1. **Drop** — отбросить пакет, в котором найдена данная сигнатура
2. **Reject-sender** — в случае если сигнатура найдена в TCP пакете, то источнику пакета отправляется пакет с установленным флагом RST (разрыв соединения), в случае если это UDP или ICMP пакет, то источнику отправляется ICMP-пакет «unreachable»
3. **Reject-reciever** — в случае если сигнатура найдена в TCP пакете, то получателю пакета отправляется пакет с установленным флагом RST (разрыв соединения), в случае если это UDP или ICMP пакет, то zywall не производит никаких действий.
4. **Reject-both** — в случае если сигнатура найдена в TCP пакете, то источнику и получателю пакета отправляется пакет с установленным флагом RST (разрыв соединения), в случае если

это UDP или ICMP пакет, то источнику отправляется ICMP-пакет «unreachable».

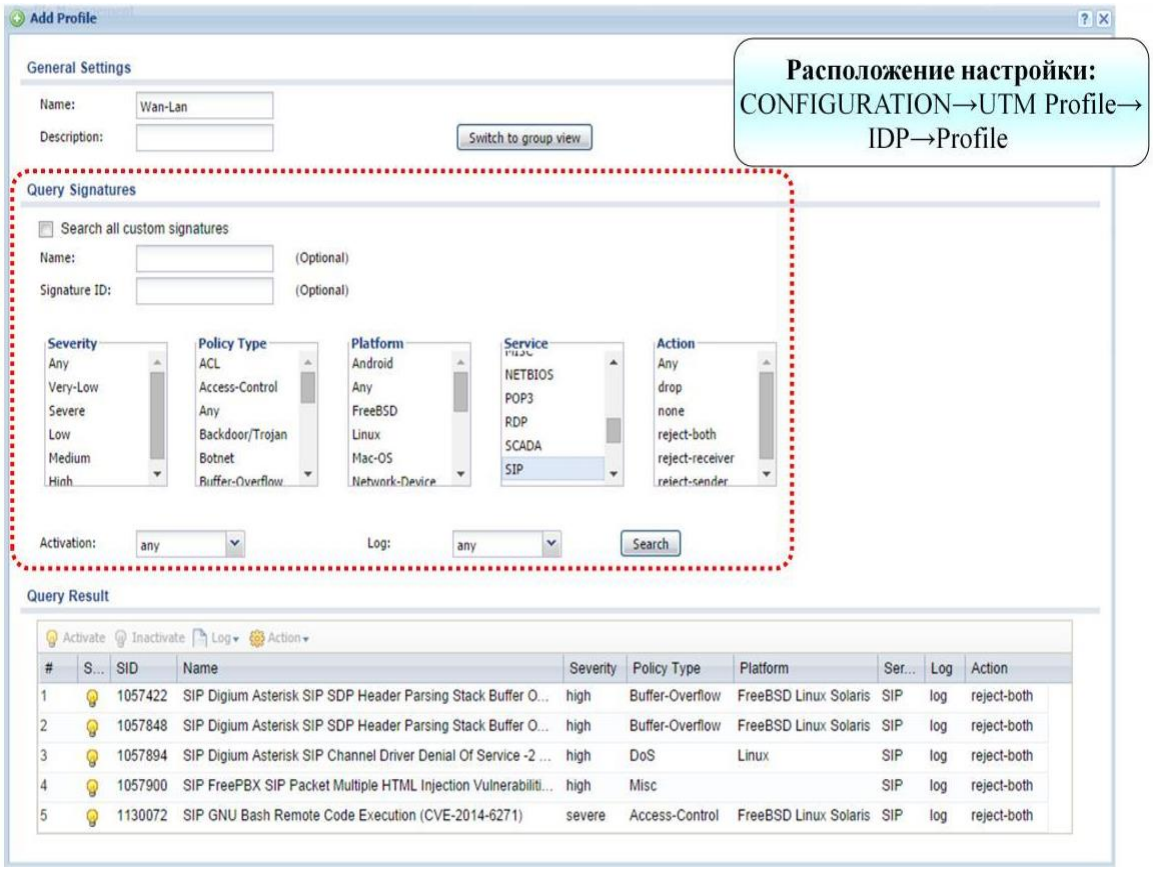


Рис. 34. Профиль IDP

SSL Inspection

SSL Inspection быстро становится необходим, так как веб-ресурсы переходят на использование зашифрованных сессий.

Например, Facebook и Gmail являются одними из популярных сайтов, предлагающих пользователям возможность шифровать их сеансы.

Этот трафик проходит без контроля через политики безопасности и функции предотвращения угроз.

SSL Inspection расшифровывает пакеты и проверяет их функциями UTM.

Если трафик попадает под действия правил UTM, то принимаются меры.

Если трафик не попадает под действия правил UTM, SSL Inspection шифрует пакеты, а затем передает их.

Клиент на рис. 32. открывает соединение SSL → ZyWALL проверяет поддержку алгоритма → ZyWALL отправляет запросы на сервер от своего имени.

Сервер отправляет сертификат на ZyWALL → ZyWALL извлекает открытый ключ сервера из сертификата → ZyWALL эмулирует сертификат для клиента.

Клиенты аутентифицируются с ZyWALL, и ZyWALL также полностью прошел проверку подлинности с сервером. ZyWALL выступает в данном случае как "человек-посередине".

В настоящее время поддерживается SSLv3 / TLS1.0.
Для трафика SSLv2 можно выбрать одно из действий: пропустить или заблокировать.

Рис. 32. Порядок работы с сертификатами

Неподдерживаемые алгоритмы защищенного подключения могут быть также пропущены или заблокированы.
В целях соблюдения необходимой конфиденциальности сотрудников предприятия доверенные интернет-ресурсы, например, такие как интернет-банки, медицинские учреждения, электронные сервисы правительства и т.п., могут быть занесены в специальный список, чтобы исключить дешифрование и инспектирование трафика пользователей этих ресурсов.
Если включить функцию сбора статистики, устройство будет хранить все сертификаты веб-сайтов.
Включение сбора статистики является хорошим инструментом для сетевых администраторов.
После включения SSL Inspection можно проанализировать трафик и использовать различные средства, позволяющие заблокировать нежелательные службы.
Существует ограничение "maximum concurrent session", которое является ограничением сессий для функции SSL Inspection.

Anti-Virus

Функция Anti-Virus на устройствах серий ZyWALL и USG позволяет проверять наличие известных сигнатур в пакетах протоколов HTTP/FTP/SMTP/POP3/IMAP4.

В качестве поставщика сигнатур используют компанию «Лаборатория Касперского».

Поддерживаются алгоритмы архивации: ZIP/RAR.

Функция Anti-Virus работает на базе правил, которые можно привязать к различным направлениям в Unified Security Policy, то есть наличие проверки потока пакетов на вирусы или ее отсутствие определяется направлением движения трафика.

Поддерживаются одноуровневые архивы для сканирования, и всегда выполняется полное скачивание, а не инкрементное сканирование.

Поддерживается создание белых/черных списков файлов.

Просмотреть сигнатуры можно в журнале Anti-Virus.

AppPatrol (Application Patrol)

AppPatrol (Application Patrol) — функция, которая позволяет управлять использованием полосы пропускания устройства, а также управлять возможностью передачи определенного типа трафика (рис. 35).

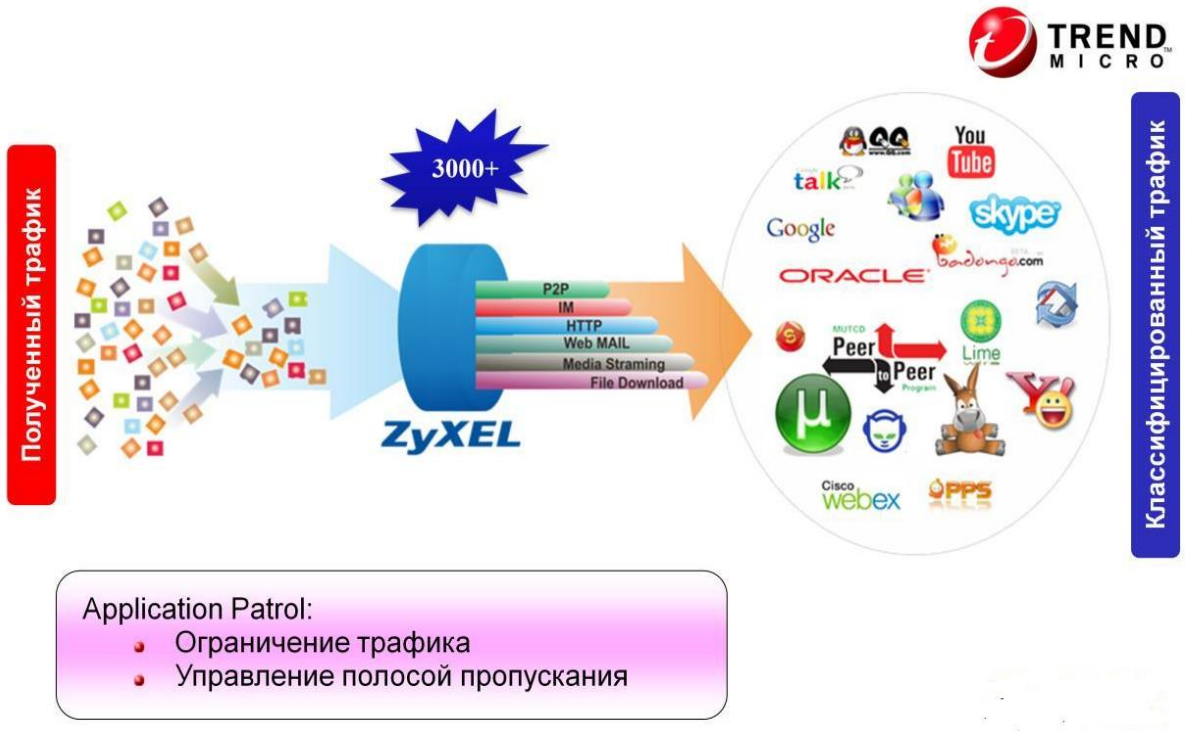


Рис. 35. AppPatrol (Application Patrol)

В качестве критериев для определения трафика можно использовать как 4 уровень OSI (TCP/UDP порты), так и вышестоящие уровни, вплоть до 7 уровня модели OSI.

Таким образом, AppPatrol позволяет ограничивать передачу или управлять полосой пропускания практически для любого типа трафика, включая irc, icq, jabber, torrent, edonkey и т.д.

AppPatrol, не единственная функция, способная управлять полосой пропускания устройства, это умеет и функция Policy Routing, причем правила, описанные в Policy Routing, имеют больший приоритет, нежели правила, описанные в AppPatrol.

Функция AppPatrol может смотреть в пакет гораздо глубже (до 7 уровня OSI) нежели Policy Routing (4 уровень OSI), поэтому для управления полосой пропускания трафика, который идет поверх TCP и UDP, рекомендуется использовать AppPatrol, а для управления полосой пропускания трафика ICMP использовать Policy Routing.

AppPatrol позволяет ограничивать передачу какого-либо типа трафика, однако ту же функцию выполняет и Firewall, при этом трафик в первую очередь обрабатывается функцией Firewall и только после этого функцией AppPatrol.

Система управления сетевыми приложениями (Application Intelligence) от компании TREND Micro способна идентифицировать трафик более чем 3000 популярных сетевых приложений, принадлежащих к различным категориям.

Правила Application Intelligence, создаваемые IT-персоналом, позволяют с легкостью управлять трафиком приложений, запрещать трафик /разрешать/ограничивать полосу пропускания/собирать статистику для определенных пользователей/групп пользователей/хостов/диапазонов IPадресов/подсетей и, при необходимости, активировать/деактивировать правила в определенное время, по расписанию. Application Intelligence является простым и эффективным инструментом в руках IT-персонала предприятия.

С его помощью можно ограничить трафик нежелательных, небезопасных и не имеющих отношения к рабочему процессу приложений и одновременно с этим обеспечить гарантированную полосу пропускания для полезного трафика, повышая тем самым безопасность корпоративной сети и продуктивность рабочего процесса.

При создании профиля можно выбрать не только конкретные сервисы, но и различные действия, относящиеся к работе этого сервиса.

Например, можно запретить пользователю проявлять различную активность (писать сообщения, смотреть видео и т.д.), но не блокировать полностью ресурс.

Content Filtering

Реализация фильтрации по содержанию использует следующие возможности.

Black List — механизм, с помощью которого администратор может определить список запрещенных для посещения сайтов, соответственно все остальные сайты (не находящиеся в Black List) доступны для посещения.

White List — механизм, с помощью которого администратор может определить список разрешенных для посещения сайтов, соответственно все остальные сайты (не находящиеся в White List) недоступны для посещения.

URL Keyword — механизм, с помощью которого администратор может определить список ключевых слов (комбинаций символов), и в случае, если в адресе сайта, на который отправлен запрос, данная комбинация присутствует, то запрос будет заблокирован.

Category Block — функция, которая позволяет блокировать запросы пользователей по принципу того, к какой категории относится запрашиваемая страница. Все сайты разделены на различные категории.

Алгоритм работы Category Block следующий:

1. Пользователь отправляет HTTP GET запрос, так как ZyWALL является шлюзом, значит этот запрос пройдет через него.
2. ZyWALL отправляет запрос на сервер компании CYREN.
3. Сервер CYREN отвечает на запрос, сообщая, к какой категории относится данный веб-сайт.
4. ZyWALL добавляет запись в кеш, что сайт news.com относится к категории новости (данная запись будет использоваться при повторных запросах).
5. ZyWALL проверяет политики безопасности, и соответственно, в случае если пользователь имеет право посещать страницы из данной категории, HTTP GET запрос перенаправляется на адрес назначения, в случае если пользователь не имеет права посещать страницы из данной категории, ZyWALL отправляет пользователю ответ, что страницы данной категории запрещены для просмотра.

В случае если пользователь не имеет права просматривать веб-сайты из данного раздела, то он увидит в браузере сообщение об этом, содержание сообщения задает администратор (строка 255 символов).

Также дополнительно в отдельном фрейме пользователь может увидеть страницу, определенную администратором.

Например, пользователь может увидеть страницу с формой, заполнив которую пользователь отсылает письмо администратору с описанием причины, по которой данный сайт должен быть открыт для просмотра.

Алгоритм (рис. 36) работы контентной фильтрации следующий:

1. HTTP GET запрос приходит на ZyWALL.
2. В зависимости от времени суток, дня недели, адреса источника HTTP GET запроса и имени пользователя, данный запрос будет обрабатываться одной из созданных политик контентной фильтрации. В случае, если запрос не подпадает ни под одну политику, будет произведено действие по умолчания (Forward или Block).
3. В случае, если запрос попадает под какую-то политику безопасности, то в первую очередь будет проверяться наличие адреса назначения в Black List, если адрес присутствует, то запрос будет заблокирован, если нет, то будет обрабатываться списком URL Keyword List.

4. Следующим шагом проверяется наличие слов из URL Keyword List в адресе назначения. Если слова из данного списка присутствуют в адресе назначения, то будет произведена проверка с помощью White List. Если адрес данного веб-узла присутствует в White List, то запрос будет отправлен, если нет, то заблокирован.

После проверки с помощью URL Keyword List производится определение категории, к которой относится данный сайт, и если сайт относится к разрешенной категории, то запрос перенаправляется.

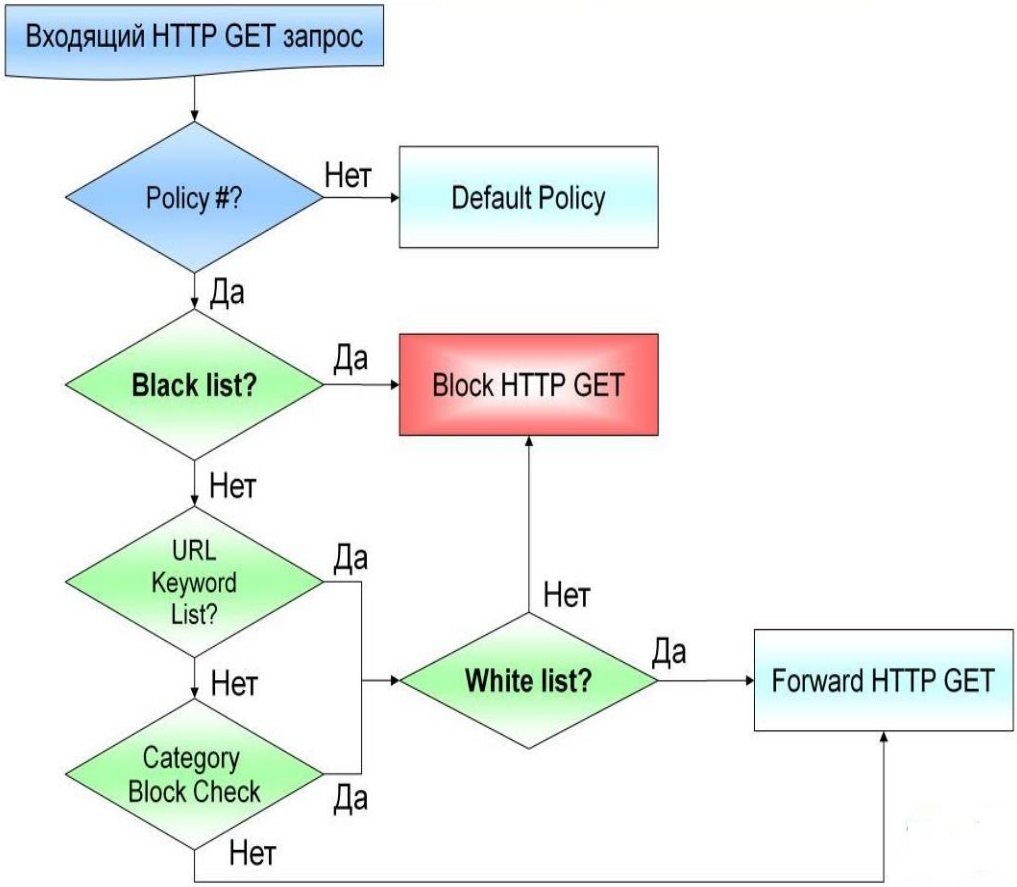


Рис. 36. Общая схема работы контентной фильтрации

Если сайт относится к запрещенной категории, то будет произведена проверка с помощью White List. Если адрес данного веб-узла присутствует в White List, то запрос будет отправлен, если нет, то заблокирован.

Сервис контентной фильтрации в операционной системе ZLD 4.10 использует доступ к облачной базе данных компании CYREN — ведущего поставщика интегрированных облачных решений и ПО для создания систем безопасности. Эта постоянно обновляемая база данных позволяет классифицировать более 140 биллионов веб-сайтов, разделяя их на 64 категории — от “бизнеса и экономики” до “игр” и “спорта”, включая восемь потенциально опасных (Anonymizers, Malware, Phishing&Fraud, Botnets, Network Errors, Spam Sites, Compromised и Parked Domains).

Сервис контентной фильтрации анализирует HTTP-запрос от пользователя на соединение с тем или иным интернет-сайтом, запрашивая категорию сайта в

базе данных SYREN. Гибкий механизм правил контентной фильтрации позволяет разрешать или запрещать доступ к определенным категориям сайтов для определенных пользователей или групп пользователей, разрешать доступ к любым ресурсам Интернета без ограничений для привилегированных пользователей, а также активировать правила контентной фильтрации по расписанию в определенный период времени, например, в рабочее время. Запросы пользователей, направляемые к сайтам из запрещенных категорий, блокируются с возвратом специального предупреждения и занесением информации в системный лог устройства, позволяя IT-специалистам компании получать статистику по пользователям и запрашиваемым ими веб-ресурсам.
Благодаря сервису контентной фильтрации (Content Filtering) IT специалисты могут ограничивать доступ сотрудников к интернет-ресурсам, не имеющим отношения к рабочим вопросам, а также исключать доступ к потенциально опасным ресурсам, тем самым повышая продуктивность работы сотрудников, освобождая каналы подключения к Интернету от нежелательного трафика и повышая уровень сетевой безопасности.
Настройка профиля: Category Service включает в себя следующие поля.

1. Action for Unsafe Web Pages — небезопасные сайты (Вредоносные, Фишинг и мошенничество, Бот-сети, Спам сайты).
2. Action for Managed Web Pages — сайты из категорий.
3. Action for Unrated Web Pages — сайты не попавшие в категории.

Действия:

1. Pass — дать доступ
2. Warm — дать доступ, но предупредить
3. Block — заблокировать

Настройка профиля может быть выборочной в меню Custom Service.

Статистику работы можно увидеть в личном кабинете.

Антиспам

Спам (англ. spam) — массовая неперсонифицированная, рассылка с использованием специальных программ, коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать.
Функция Anti-Spam на устройствах серий ZyWALL и USG позволяет обрабатывать трафик SMTP (TCP порт #25) и POP3 (TCP порт #110) протоколов, остальные протоколы, например, IMAP не поддерживаются. Решение о том, является ли данное письмо спамом или нет, может приниматься с помощью трех функций:

1. White and Black List
2. DNSBL (DNS Block List или DNS Black List)
3. Scan Server

Существует ряд действий, которые ZyWALL может произвести с письмами, которые он определил, как спам-сообщения:

1. пропустить письмо
2. отбросить письмо
3. пропустить письмо, однако изменить тему письмо, например, добавить тег [SPAM].

Black List — набор правил, которые позволяют определить письмо как спам-сообщение, в качестве критериев могут выступать любые поля E-mail Header.
White List — набор правил, которые позволяют определить письмо как не спам-сообщение, в качестве критериев могут выступать любые поля E-mail Header.
DNSBL (DNS BlackList или DNS BlockList) — списки хостов, хранимые с использованием системы архитектуры DNS. В данном случае используются для борьбы со спамом.
DNSBL сервера хранят следующую информацию:

1. адреса открытых релеев, то есть адреса неправильно настроенных почтовых серверов, которые позволяют пересылать через себя почтовые сообщения для всех желающих. Как правило данные хосты автоматически сканируются в Интернете, поэтому попадание такого хоста в руки людей, рассылающих спам, происходит очень быстро (не более 4 дней)
2. адреса спам-серверов, то есть адреса хостов, через которые было замечено прохождение спам-сообщений. Данные списки составляются на основе показаний пользователей
3. адреса открытых HTTP/Socks прокси-серверов, позволяющих без контроля доступа любому пользователю совершать неавторизованные действия, скрывая свой реальный IP адрес

Таким образом, ZyWALL может использовать DNSBL сервера для определения, является ли данное письмо спамом или нет.
В случае если все DNSBL сервера недоступны в течение определенного тайм-аута (задается администратором), ZyWALL выполнит одно из трех возможных действий с письмом согласно настройкам.
Алгоритм (рис. 37) работы функции Anti-Spam следующий:

1. Письмо приходит на ZyWALL
2. ZyWALL проверяет, надо ли применять функцию anti-spam на данном направлении, направление определяется зоной источника и зоной назначения. В случае если на данном направлении anti-spam применять не надо, письмо отправляется.
3. В случае если на данном направлении письмо необходимо обработать Anti-Spam, то проверяется не подпадает ли это письмо под правила White List, если подпадает, то письмо пересылается.
4. Если письмо не попадает под действия правила White List, то проверятся, попадает ли оно под действия правила Black List, если попадает, значит, данное письмо является спамом, и выполняется соответствующее действие.

5. Если письмо не попадает под действия правила Black List, то проверяется IP-адрес источника с помощью DNSBL серверов. Если механизм DNSBL подтверждает наличие IP-адреса источника в своей базе, это означает, что письмо является спамом, и выполняется соответствующее действие. Если данный IP-адрес источника не содержится в базах DNSBL серверов, это означает, что данное письмо не является спам-сообщением, и оно пересылается. В случае если DNSBL сервера не отвечают в течение указанного тайм-аута, то выполняется соответствующее действие с письмом.

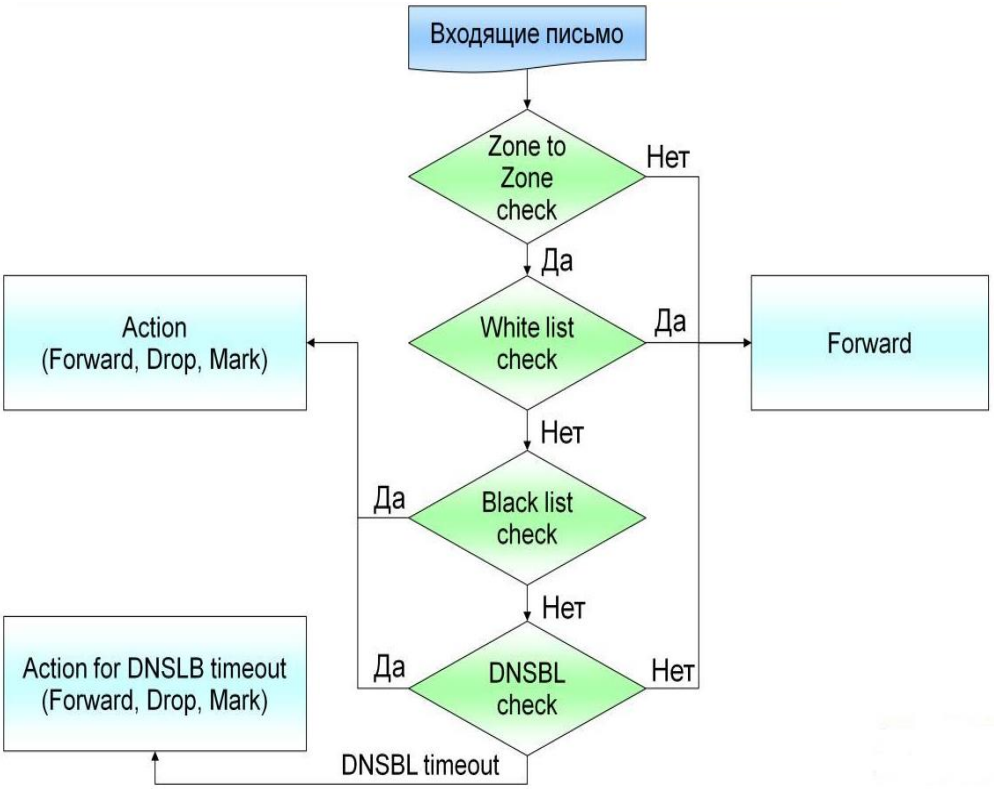


Рис. 37. Общая съема работы Anti-Spam

CYREN Scan Server

Проверка писем при помощи CYREN осуществляется на наличие спама и вирусов.

При проверке, сначала просматривается локальный кэш устройства, в случае если информация в нем отсутствует, то происходит обращение к серверу, после чего информация будет записана в локальный кэш.

По данным статистики Лаборатории Касперского, наибольшее количество спама приходится на письма объемом данных менее 5 кб, и также небольшое количество – на письма объемом 5-50 кб.

В зависимости от модели ZyWALL USG устройство может отправить на анализ в CYREN небольшую часть письма. Этого достаточно, чтобы с очень высокой вероятностью проанализировать наличие спама в письме.

Основные преимущества функции антиспам:

1. эффективное обнаружение спама независимо от формата, языка и кодировки сообщений;
2. идентификация новых спам-рассылок через считаные минуты после их инициализации;
3. технология CYREN успешно различает полезные, ожидаемые пользователями массовые рассылки от спама;
4. раннее обнаружение новых вирусов, троянов и других вредоносных программ, распространяемых спамерами;
5. весь спам может фильтроваться на границе сети, не доходя до почтового сервера и тем самым не перегружая его;
6. защита от фишинга. Блокируются электронные сообщения от интернет-мошенников, пытающихся завладеть конфиденциальной информацией.

Фильтрация по репутации IP-адреса отправителя (Sender-Based IP Reputation Filter). ZyWALL выявляет до 80% спама, тем самым значительно сокращая интернет-трафик и потребление системных ресурсов на втором и третьем этапе фильтрации.

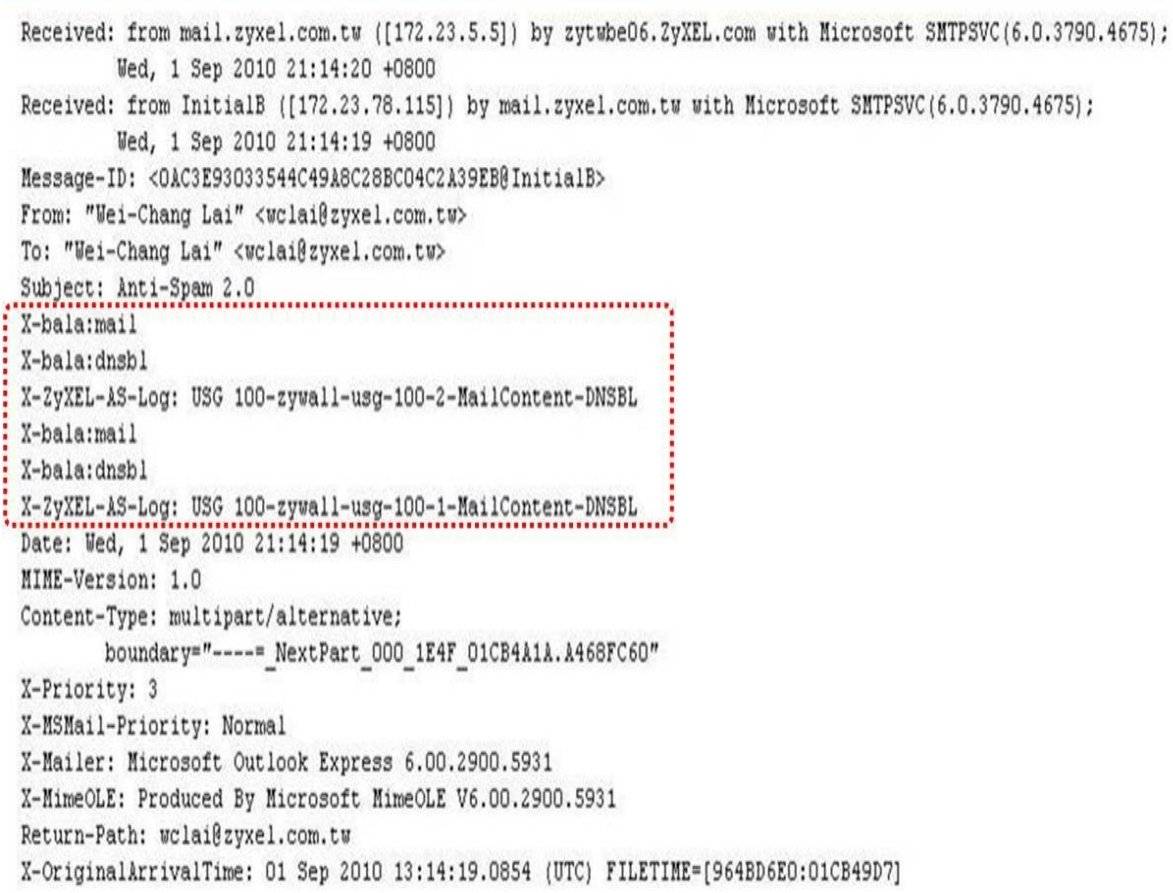


Рис. 38. X-Header

Фильтрация по повторяющимся шаблонам (Recurrent Pattern Detection или RPD) — общим характерным признакам (шаблонам), присущим сообщениям каждой

спам-рассылки, например, таким как URL коммерческих сайтов, текстовые последовательности, файлы во вложении, а также количество отправленных сообщений в единицу времени, адреса отправителей и получателей.
Этот тип фильтрации позволяет отфильтровывать до 99 процентов спама.
Антивирусная проверка вложений с технологией Zero-hour Virus Outbreak использует облачную базу данных вирусных сигнатур.
В случае обнаружения во вложении сообщения подозрительного файла, для которого отсутствует сигнатура в базе данных, устройство ZyWALL задерживает сообщение на час.
В течение часа сервер анализирует подозрительный файл и возвращает устройству окончательный ответ о том, является ли файл вредоносным, пополняя при этом (при необходимости) свою базу новой сигнатурой.
Дополнительный заголовок X-Header (рис. 38) не виден по умолчанию пользователю, но может быть дополнительной полезной информацией для обработки локальным почтовым сервером.
Статистику работы функции Anti-Spam можно просматривать на самом ZyWALL, также возможна отправка этой статистики на электронную почту администратора (меню Maintenance — Report — Email Daily report).

BWM

Функция BWM (bandwidth management) в ZyWALL USG позволяет распределять общую пропускную полосу по настроенным критериям.
BWM работает в зависимости от направления сессии по интерфейсам.
Таким образом, в настройках правила IP-адрес источника (Source) - это IP-адрес инициатора сессии, а IP-адрес назначения (Destination) - это IP-адрес, на который сессия открывается.
Входящий/Исходящий (inbound/outbound) трафик считается по отношению к инициатору сессии.
Инициатор сессии посылает outbound(исходящий) трафик и принимает inbound (входящий) трафик.
Для outbound (исходящего) трафика правила BWM применяются перед отправкой пакета на вышестоящий шлюз.
Для inbound (входящего) трафика правила BWM применяются перед отправкой инициатору сессии.
Настройки BWM для Policy Route и App Patrol централизованы в общие настройки BWM.
Управление скоростью входящего и исходящего трафика в одном правиле следующие:
Трафик inbound: Инициатор → Получатель
Трафик outbound: Получатель → Инициатор
Настройка BWM показана на рис. 39 и включает в себя указание поля Service Type (Тип сервиса):
Service Object – здесь можно выбрать объект Service (Configuration > Object > Service), который содержит протокол и номер порта.

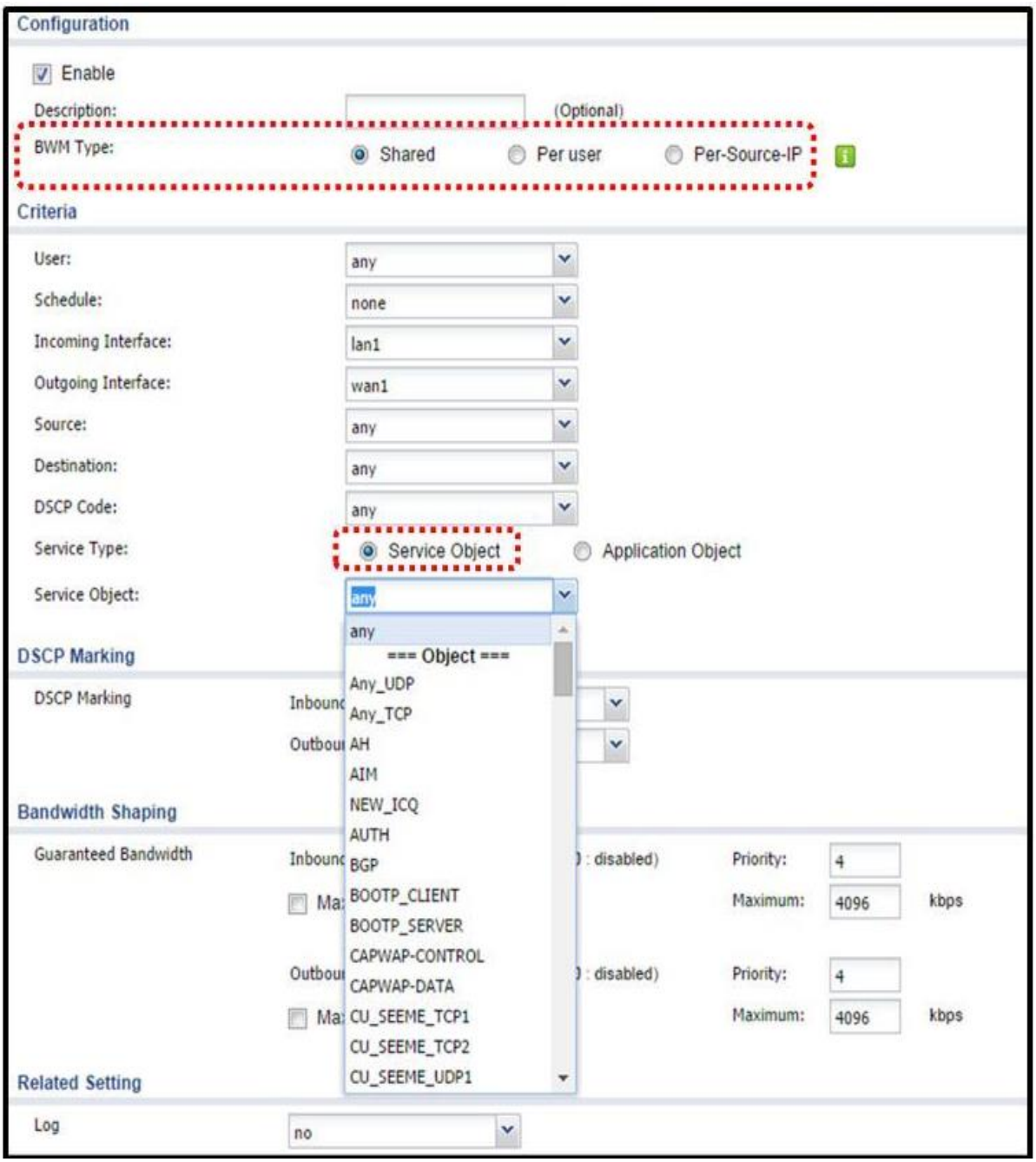


Рис. 39. Настройка BWM

App Patrol Service - это объект Aplication Patrol (сигнатуры App Patrol обновляются вместе с IDP - это платная подписка на 1-2 года), который может выявлять определенный сервис или приложения по сигнатурам.

Настройка Bandwidth показана на рис. 39 и включает заполнение следующих полей.

Guaranteed Bandwidth – гарантированная полоса пропускания.

Для входящего по отношению к устройству трафика Inbound:

Inbound – значения гарантированной полосы пропускания для входящего трафика.

Priority – приоритет для входящего трафика.

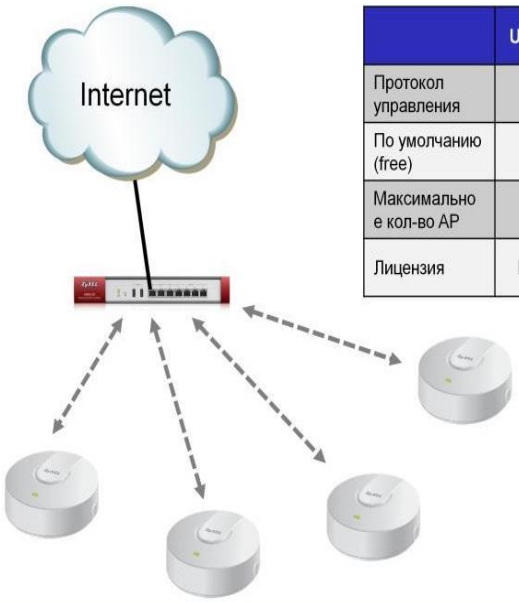
Maximum – максимальная полоса для входящего трафика по данному правилу. Неактивна, если используется Maximize Bandwidth Usage (в этом случае максимальная полоса не ограничивается).
Maximize Bandwidth Usage - при включении позволяет правилу использовать всю незадействованную полосу.
Для исходящего по отношению к устройству трафика Outbound:
Outbound – значения гарантированной полосы пропускания для исходящего трафика.
Priority – приоритет для исходящего трафика.
Maximum – максимальная полоса для исходящего трафика по данному правилу. Неактивна, если используется Maximize Bandwidth Usage (в этом случае максимальная полоса не ограничивается).
Maximize Bandwidth Usage - при включении позволяет правилу использовать всю незадействованную полосу.

Контроллер WLAN

Встроенный контроллер WLAN предлагается на всех моделях устройств ZyWALL и USG.
Все модели могут контролировать 2 точки беспроводного доступа по умолчанию.
Если нужно управлять большим количеством точек, то требуется приобрести дополнительную лицензию.
Одна лицензия добавляет 8 точек доступа.
Максимальное количество точек доступа для каждого устройства приведено на рис. 40.
Поддерживаемые функции:

1. DCS (Dynamic Channel Selection)
2. Layer 2 Isolation
3. Client Steering
4. AP Load Balancing
5. Auto Healing
6. Monitor Mode/Rogue AP Management
7. Wireless Frame Capture
8. Wireless Schedule On/Off

Для настройки точки доступа в режиме Access Point необходимо создать радио-профиль, в котором указать физические параметры работы радио-интерфейса (стандарт 802.11 и рабочую частоту), выбрать предварительно настроенные профили SSID, а также настроить другие параметры, которые при необходимости отображаются в продвинутом интерфейсе.
После настройки радио-профиля радио-интерфейс точки доступа переключается в режим Access Point и указывается соответствующий радио-профиль.



	USG40(W)	USG60(W)	ZyWALL 110	ZyWALL 310	ZyWALL 1100
Протокол управления	CAPWAP				
По умолчанию (free)	2	2	2	2	2
Максимально е кол-во AP	10	10	18	18	18
Лицензия	По 8 шт.	По 8 шт.	По 8 шт.	По 8 шт.	По 8 шт.

Серия	NWA3000-N Series	NWA5000 Series	NWA5120 Series
Модель	NWA3160-N NWA3560-N NWA3550-N	NWA5160-N NWA5560-N NWA5550-N	NWA5121-NI NWA5121-N NWA5123-NI

Рис. 40. Встроенный контроллер WLAN

В дальнейшем все настройки, мониторинг и управление точкой доступа производится через веб-интерфейс ZyWALL.

Контрольные вопросы

1. Каково назначение Unified Security Policy?
2. Каково назначение Firewall?
3. Каково назначение ADP?
4. Каково назначение SSL Inspection?
5. Каково назначение Anti-virus?
6. Каково назначение IDP?
7. Каково назначение Application Patrol?
8. Каково назначение Content Filtering?
9. Каково назначение Anti-spam?
10. Каково назначение BWM?
11. Каково назначение WLAN Controller?

Приложение

Packet Flow

Условные обозначения:

Ethernet	Ethernet интерфейс получения/отправки пакета
VLAN	VLAN
Encap	PPPoE или PPTP инкапсуляция

ALG	Application Layer Gateway
DNAT	Destination NAT
Routing	Маршрутизация, включая политики маршрутизации, статические маршруты, балансировку нагрузки и т.д.
FW	Firewall, для пакетов проходящих через ZyWALL
zFW	Firewall, для пакетов, предназначены для самого ZyWALL
IDP	Intrusion Detection and Protection
ADP	Anomaly Detection and Protection
AP	Application Patrol
AS	Anti-Spam
CF	Content Filtering
SNAT	Source NAT
IPSec D/E	IPSec VPN Decryption/Encryption
BWM	Bandwidth Management
RM	Remote Management
AV	Anti-Virus

Последовательность работы функций при прохождении пакета из одного интерфейса ZyWALL в другой:
Ethernet → VLAN → Encap → ALG → DNAT → Routing → FW → IDP → AP → CF → AV → AS → SNAT → BWM → Encap → VLAN → Ethernet

Последовательность работы функций при прохождении пакета из одного интерфейса ZyWALL до самого ZyWALL, и от ZyWALL наружу через какой-либо интерфейс:
К ZyWALL: Ethernet → VLAN → Encap → ALG → DNAT → Routing → zFW → ADP → RM
От ZyWALL: RM → Routing → BWM → Encap → VLAN → Ethernet

Последовательность работы функций при прохождении пакета из какого-либо интерфейса через ZyWALL в VPN туннель:
Ethernet → VLAN → Encap → ALG → DNAT → Routing → FW → IDP → AP → CF → AV → AS → SNAT → IPSec E → Routing → BWM → Encap → VLAN → Ethernet

Последовательность работы функций при прохождении пакета из VPN туннеля в какойлибо интерфейс ZyWALL:
Ethernet → VLAN → Encap → ALG → DNAT → Routing → zFW → IPSec D → ALG → AC → DNAT → Routing → FW → IDP → AP → CF → AV → AS → SNAT → IPSec E → Routing → BWM → Encap → VLAN → Ethernet

Глоссарий

AD (Active Directory) - LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT.
AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), финалист конкурса AES и принятый в качестве американского стандарта шифрования правительством США.
AH (Authentication Header) — один из протоколов IPSec, позволяющий обеспечить аутентификацию источника, целостность данных, а также защиту от повторной передачи. Данный алгоритм не обеспечивает шифрования. (RFC 2402, RFC 4302)
ASAS (Authenex Strong Authentication Server) — RADIUS-сервер, используется для двухфакторной аутентификации.
DES (Data Encryption Standart) — симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для дешифровки данных. DES разработан фирмой IBM. Для шифрования использует ключ с длиной 56 бит.
3DES (Triple Data Encryption Standart) — симметричный алгоритм, созданный Whitfield Deffie, Martin Hellman, Walt tuchmann в 1978г. на основе алгоритма DES с целью устранения главного недостатка последнего — малой длины ключа (56 бит). Алгоритм 3DES работает в 3 раза медленнее, чем DES, но криптостойкость намного выше.
Device HA (Device High Availability) — функция, которая позволяет использовать несколько устройств серии ZyWALL USG в качестве шлюза, тем самым обеспечивание резервирование.
DH (Diffie-Hellman) — алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования. (RFC 2631).
DPD (Dead Peer Detecrion) — механизм, с помощью которого IPSec VPN шлюз может проверить работоспособность удаленного шлюза безопасности. (RFC 3706).
DSA (Digital Signature Algorithm) — асимметричный алгоритм с использованием открытого ключа и секретного ключа, применяется для создания электронной подписи, но не для шифрования
ESP (Encapsulationg Security Payload) — один из протоколов IPSec, позволяющий обеспечить аутентификацию источника, целостность данных,

защиту от повторной передачи, а также шифрование данных. (RFC 2406, RFC 4303)

HMAC (Hash Message Authentication Code) — математическая функция, алгоритм которой чаще всего базируется на алгоритме MD5 или SHA-1, однако при расчете хешкода используется дополнительный параметр — секретный ключ. (RFC 2104, RFC 2403, RFC 4304)

ICV (Integrity check value) — контрольная сумма, некоторое значение, рассчитанное путём применения определённых операций над входными данными. То же самое, что и хеш-код.

IKE (Internet Key Exchange) — один из протоколов IPSec обеспечивающий согласование параметров ассоциаций защиты (SA) IKE и IPSec, а также выбор ключей для алгоритмов шифрования, используемых в рамках IPSec. (RFC 2409, RFC 4306)

IPsec (IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. (RFC 2401, RFC 4301)

LDAP (Lightweight Directory Access Protocol — «облегчённый протокол доступа к каталогам») - это сетевой протокол для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP. (RFC 4510 — RFC 4521)

MAC (Message Authentication Code) — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных.

MD5 (Message Digest 5) — 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского Технологического Института (MIT, Massachusetts Institute of Technlogy) в 1991 году. Предназначен для создания «хешкодов» или «дайджестов» сообщений произвольной длины. (RFC 1321)

NAS (Network Access Server) — устройство доступа к сети, в контексте решения двухфакторной аутентификации ZyXEL — это шлюз ZyWALL.

NAT (Network Address Translation) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса проходящих пакетов. (RFC 1631, RFC 3022)

NAPT (Network Address Port Translation) — частный случай механизма NAT, который помимо подмены IP-адресов проходящих пакетов обеспечивает подмену TCP/UDP портов проходящих пакетов. (RFC 3022)

NAT-T (NAT Traversal) — механизм, с помощью которого возможна установка и использование IPSec VPN туннеля по протоколу ESP в случае, если между шлюзами безопасности присутствует NAPT. (RFC 3947, RFC 3948)

OTP (One Time Password) — пароль, который может быть использован только один раз.

PFS (Perfect Forward Secrecy) — функция, позволяющая произвести дополнительный обмен по алгоритму Диффи-Хеллмана на второй стадии IKE, тем самым получая новые ключи для шифрования и аутентификации трафика при передаче по протоколам ESP или AH, которые не будут зависеть от ключей, используемых для защиты трафика IKE.
RADIUS (Remote Authentication in Dial-In User Service) - протокол AAA (Authentication, Authorization и Accounting), разработанный для передачи сведений между центральной платформой AAA и оборудованием Dial-Up доступа (NAS, Network Access Server) и системой биллинга). (RFC 2865, RFC 2866)
RSA (Rivest-Shamir-Adleman) — асимметричный алгоритм шифрования, использующий два ключа (публичный и частный), публичный ключ можно передавать в открытом виде, секретный ключ не передается вообще. Используется не только для шифрования, но и для цифровой подписи. (RFC 2313, RFC 2437)
SA (Security Association) — ассоциации защиты, представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон. Составляющими такой политики может быть алгоритм шифрования, алгоритм аутентификации и т.д.
SHA-1 (Secure Hash Algorithm 1) — алгоритм криптографического хеширования. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хешзначение, называемое также дайджестом или хеш-кодом сообщения. (RFC 3174)
SSL (Secure Socket Layer) — криптографический протокол, обеспечивающий безопасную передачу данных по публичным сетям, является альтернативой протоколу IPSec, часто применяется для организации защищенного канала между удаленным пользователем и внутренними ресурсами локальной сети.
VPN (Virtual Private Network) — логическая сеть, создаваемая поверх другой сети, например Интернет, однако обеспечивающая безопасность передачи данных.

Список литературы

1. Федорова, В.А. Проектирование физического и канального уровней безопасной вычислительной сети предприятия [Электронный ресурс]: учебное пособие / В.А. Федорова. — Электрон. дан. — Москва: МГТУ им. Н.Э. Баумана, 2017. — 20 с. — Режим доступа: https://e.lanbook.com/book/103526. — Загл. с экрана.
2. Технологии защиты информации в компьютерных сетях [Электронный ресурс] : учебное пособие / Н.А. Руденков [и др.]. — Электрон. дан. — Москва: , 2016. — 368 с. — Режим доступа: https://e.lanbook.com/book/100522. — Загл. с экрана.
3. Сайт производителя сетевого оборудования Zyxel. [Электронный ресурс]. — Режим доступа: www.zyxel.ru

4. Платунова С.М. Применение межсетевых экранов фирмы ZyXEL в корпоративных сетях. Учебное пособие по дисциплинам «Сети ЭВМ и телекоммуникации», «Защита информации в сетях». - Санкт-Петербург: Университет ИТМО, 2015. - 62 с. - экз.
5. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва: ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032. — Загл. с экрана.
6. Платунова, С.М. Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности [Электронный ресурс]: учебное пособие / С.М. Платунова. — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2012. — 85 с. — Режим доступа: https://e.lanbook.com/book/70999. — Загл. с экрана.

Платунова Светлана Михайловна
Елисеев Игорь Владимирович
Авксентьева Елена Юрьевна

Реализация комплексной безопасности в корпоративных сетях. Шлюз безопасности как универсальное средство для обеспечения защиты данных и предотвращения вторжений

Учебно-методическое пособие

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49