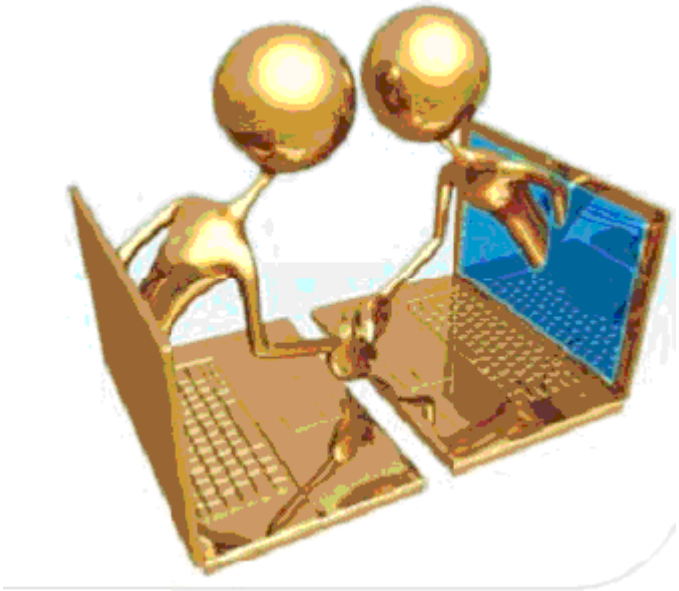
УНИВЕРСИТЕТ ИТМО

С.М. Платунова

Применение межсетевых экранов фирмы ZyXEL в корпоративных сетях

Учебное пособие



Санкт-Петербург

2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

С.М. Платунова

ПРИМЕНЕНИЕ МЕЖСЕТЕВЫХ ЭКРАНОВ ФИРМЫ ZYXEL В КОРПОРАТИВНЫХ СЕТЯХ.

Учебное пособие

Санкт-Петербург

2015

Платунова С.М. Применение межсетевых экранов фирмы ZyXEL в корпоративных сетях. Учебное пособие по дисциплинам «Сети ЭВМ и телекоммуникации», «Защита информации в сетях». – СПб: НИУ ИТМО, 2015. – 62 с.

В учебном пособии описаны общие принципы построения вычислительных сетей, стандарты построения сетей, протоколы стека TCP/IP, протоколы маршрутизации, особенности маршрутизации сетей класса SOHO, технология VPN, пример настройки оборудования фирмы ZyXEL серии ZyWALL USG.

Пособие адресовано специалистам с высшим и средним профессиональным образованием, имеющим опыт работы в области IT технологий, обучающихся по направлению/специальности: 09.04.01 «Информатика и вычислительная техника» («Системное администрирование аппаратно-программных комплексов и сетей»), 09.03.01 («Вычислительные машины, комплексы, системы и сети»).

Рекомендовано к печати Ученым советом факультета Академии ЛИМТУ, протокол № 5 от 06.11.2014

Содержание

Тема 1. Межсетевой экран

Межсетевой экран или сетевой экран - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов - динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.

Брандма́уэр (нем. Brandmauer) - заимствованный из немецкого языка термин, являющийся аналогом английского firewall в его оригинальном значении (стена, которая разделяет смежные здания, предохраняя от распространения пожара). Файрво́лл, файрво́л, файерво́л, фаерво́л - образовано транскрипцией английского термина firewall.

Разновидности сетевых экранов

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

1. обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями,
2. на уровне каких сетевых протоколов происходит контроль потока данных,
3. отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

1. традиционный сетевой (или межсетевой) экран - программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями,
2. персональный сетевой экран - программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

Вырожденный случай - использование традиционного сетевого экрана сервером, для ограничения доступа к собственным ресурсам.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие:

1. на сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором,
2. на сеансовом уровне (также известные как stateful) - отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP/IP, часто используемых в злонамеренных операциях - сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных,
3. на уровне приложений, фильтрация происходит на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Некоторые решения, относимые к сетевым экранам уровня приложения, представляют собой прокси-серверы с некоторыми возможностями сетевого экрана, реализуя прозрачные прокси-серверы, со специализацией по протоколам. Возможности прокси-сервера и многопротокольная специализация делают фильтрацию значительно более гибкой, чем на классических сетевых экранах, но такие приложения имеют все недостатки прокси-серверов (например, анонимизация трафика).

В зависимости от отслеживания активных соединений сетевые экраны бывают:

- stateless (простая фильтрация), которые не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил,
- stateful, stateful packet inspection (SPI) (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений. Такие типы сетевых экранов позволяют эффективнее бороться с различными видами DoS-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т. п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и, зачастую, несовместимых со стандартными, stateless сетевыми экранами.

Типичные возможности межсетевого экрана

Типичные возможности межсетевого экрана включают в себя:

1. фильтрация доступа к заведомо незащищенным службам,

2. препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб,
3. контроль доступа к узлам сети,
4. может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети,
5. регламентирование порядка доступа к сети,
6. уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран.

Вследствие защитных ограничений могут быть заблокированы некоторые необходимые пользователю службы, такие как Telnet, FTP, SMB, NFS, и так далее. Поэтому настройка экрана требует участия специалиста по сетевой безопасности. В противном случае вред от неправильного конфигурирования может превысить пользу.

Также следует отметить, что использование экрана увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

Проблемы, не решаемые сетевым экраном

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

1. не защищает узлы сети от проникновенisя через «люки» (англ. back doors) или уязвимости ПО,
2. не обеспечивает защиту от многих внутренних угроз, в первую очередь - утечки данных,
3. не защищает от загрузки пользователями вредоносных программ, в том числе вирусов.

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы. Обычно они подключаются к экрану и пропускают через себя соответствующую часть сетевого трафика, работая как прозрачный для прочих сетевых узлов прокси, или же получают с экрана копию всех пересылаемых данных. Однако такой анализ требует значительных аппаратных ресурсов, поэтому обычно проводится на каждом узле сети самостоятельно.

IPsec (сокращение от IP Security) - набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации vpn-соединений.

Межсетевой экран ZyWALL

Функция Firewall устройства ZyWALL включает два сервиса:

1. фильтрация пакетов, при этом устройство проверяет сетевой уровень, единицей фильтрации является пакет, администрирование производится в CLI,
2. инспекция пакетов с учетом состояния, при этом проверяет все службы, единицей фильтрации является соединение, производится в web-интерфейс.

NCSA (Национальная Ассоциация по Компьютерной Безопасности) разделяет межсетевые экраны на три типа.

1. **Фильтрация пакетов (packet filtering).** Это межсетевой экран первого поколения, реализуемый обычно маршрутизатором или UNIX-хостом. Он проверяет обслуживание на сетевом уровне,
2. **Proxy-шлюз (applicatio-level gateway).** Это межсетевой экран второго поколения, он проверяет обслуживание на уровне приложения,
3. **Проверка состояния (Stateful Inspection Firewall).** Это межсетевой экран третьего поколения, который предлагается как самый современный и надежный. Он проверяет все обслуживание на уровне протокола OSI (взаимодействие открытых систем) и является "прозрачным" для клиентов.

В общем случае все межсетевые экраны функционируют на основе информации, получаемой от различных уровней эталонной модели ISO/OSI, и чем выше уровень OSI, на основе которого построен межсетевой экран, тем выше уровень защиты, им обеспечиваемый.

Практически все предлагаемые на рынке межсетевые экраны анонсируются, как относящиеся к этой категории (Stateful Inspection Firewall).

Атаки типа DoS

Это атаки на сеть, цель которых не похитить информацию, а блокировать некоторое устройство или всю сеть так, чтобы пользователи не имели доступа к сетевым ресурсам.

Когда устройство или сеть подверглась атаке типа DoS, они могут приостановиться, аварийно завершить свою работу или перезапуститься.

Такие последствия могут быть конечной целью злоумышленника или могут являться только прелюдией к более серьезной атаке. Например, некая автоматизированная система может попытаться предпринять атаки типа DoS на смежные группы IP-адресов, а затем проверить эти адреса на отклик. Если никакого отклика от нефункционирующего надлежащим образом сервера нет (т.е. атака на сервер была успешной), данный сайт в будущем может быть подвергнут более изощренному взлому.

Правила по умолчанию

Для доступа к настройкам Firewall в Web конфигураторе необходимо перейти на соответствующую закладку.
Для включения функций Firewall необходимо установить флаг ☑ возле поля Enable firewall.
Функция Allow Asymmetrical Route отключает проверку наличия асимметричных маршрутов (Triangle Route).

Triangle Route

В идеальном варианте весь исходящий трафик из LAN в WAN проходит через ZyWALL, следовательно, происходит нормальное отслеживание состояний открытости соединений и их установлений. Если мы используем запасной шлюз, то ZyWALL получив запрос на соединение перенаправит его на запасной шлюз и внесет соответствующую запись в свой журнал. После прихода ответа на шлюз В на подтверждение соединения этот ответ будет отправлен запрашивающей машине и минует ZyWALL.
Таким образом, ZyWALL не будет знать, что соединение установлено и разорвет его путем посылки соответствующего пакета. Решить эту проблему можно тремя способами:

1. Включить функцию Allow Asymmetrical Route в настройках firewall,
2. Использование IP Alias. ZyWALL поддерживает до трех логических сетей, подключенных к локальному порту. Таким образом, необходимо IP адрес запасного шлюза назначить из другой подсети (не из той, которую использует локальная сеть) и назначить IP Alias в ZyWALL,
3. Все шлюзы необходимо подключить на WAN стороне ZyWALL.

В ZyWALL определено 16 потоков данных. По каждому потоку можно определить основную политику. В режиме моста дополнительно к логированию срабатывания основной политики можно включить логирование широковещательных кадров.
ZyWALL является четырехинтерфейсным маршрутизатором: LAN, WAN, DMZ, WLAN. С точки зрения логики устройства сам ZyWALL выступает во всех четырех интерфейсах сторонним устройством, поэтому выделены интерфейсы LAN-LAN ZyWALL, WAN-WAN ZyWALL, DMZ-DMZ ZYWALL, WLAN-WLAN ZyWALL.
По умолчанию в каждом интерфейсе может быть определено одно из трех действий по умолчанию:

1. **Drop** – отбрасывать все входящие сообщения,
2. **Reject** – отбрасывать все входящие сообщения и отправлять ICMP Unreachable ответ,
3. **Permit** – пропускать все входящие сообщения,
4. В микропрограммах версий до 4.00 включительно, данные, отправляемые в IPSec VPN, считались априори безопасными и не

проверялись ни одним из сервисов UTM (Unified). Начиная с микропрограммы 4.01, ZyWALL может быть настроен так, чтобы проверять данные, отправляемые в IPSec VPN.

Добавление правил

Правила привязываются к одному из 16 потоков. На закладке **Rule Summary** отображается сводная информация по всем правилам, определенным для выбранного направления потока данных. Любое правило можно удалить, модифицировать или передвинуть в списке.
При создании правил определяется информация для анализа (IP адресация, порты протоколов), и действие, необходимое для этого правила.
Для каждого правила можно определить расписание срабатывания по дням недели и времени (должно быть настроено время синхронизации).

Настройка Firewall

ZyWALL поддерживает функцию **anti-probing**, которая запрещает ответы на ICMP запросы к самому ZyWALL. Можно определить интерфейсы, по кторым ZyWaLL будет отвечать на входящие ping запросы.
Опция **Don’t Respond to requests for unathorized services** предотвращает возможность обнаружения ZyWALL хакерами при помощи сканирования неиспользуемых портов.
Если отметить эту опцию, то ZyWALL не будет отвечать на запросы к неиспользуемым портам, скрывая свое присутствие в сети. По умолчанию эта функция не включена и ZyWALL отвечает ICMP Port Unreachable пакетами на UDP запросы к закрытым портам и TCP Reset пакетами к соответствующим неиспользуемым TCP портам.
Все входящие пакеты должны вначале пройти политики Firewall на ZyWALL прежде чем будут обработаны anti-probing механизмом. Следовательно, если правила firewall блокируют входящий запрос, ZyWALL реагирует на это в соответствии с правилами, которые по умолчанию на TCP запрос отправляют TCP reset пакет.
Можно отключить это при помощи команды "sys firewall tcprst rst [on|off]".
При срабатывании правил firewall на блокирование входящего UDP пакета ZyWALL не отправит никакие ответные пакеты.
На закладке Threshold задаются предельные значения параметров для определения DoS атак.
Для защиты сети или сервера от атак типа DoS межсетевой экран ZyWALL использует допустимые предельные значения DoS для определения момента, когда нужно прервать сеансы связи, которые не полностью установлены.
При этом сеть будет способна надежно осуществлять обычные соединения.
Межсетевой экран раз в минуту определяет число и интенсивность полуоткрытых сеансов связи. Для протокола TCP, "полуоткрытость"

означает, что сеанс связи еще не был полностью завершен. Для протокола UDP, "полуоткрытость" означает, что межсетевой экран не обнаружил ответный трафик. Далее задаются параметры:

1. **одноминутный минимум (определяется интенсивностью связей, интенсивность** - это число новых попыток установления соединений, обнаруженных за последнюю минуту). Межсетевой экран **прекращает удаление новых** полуоткрытых сеансов связи из своей таблицы,
2. **одноминутный максимум**. Межсетевой экран **начинает удаление новых** полуоткрытых сеансов связи из своей таблицы,
3. **минимум незавершенных (определяется числом связей).** Межсетевой экран **прекращает очистку уже существующих** полуоткрытых сеансов связи из своей таблицы,
4. **максимум незавершенных (определяется числом связей).** Межсетевой экран **начинает очистку уже существующих** полуоткрытых сеансов связи из своей таблицы,
5. **максимум незавершенных по протоколу TCP и Время блокирования**. Они определяют максимально допустимое число полуоткрытых сеансов связи с данным адресатом.

Межсетевой экран удаляет полуоткрытые сеансы связи с одним и тем же адресатом в соответствии с одной из следующих установок времени блокирования:

1) Время блокирования равно 0 (нет блокирования, немедленный прием новых сеансов связи). Межсетевой экран удаляет самые старые существующие полуоткрытые сеансы связи с данным хостом, чтобы допустить новые запросы на соединения. В этом случае количество полуоткрытых соединений для данного хоста не может превысить допустимый предел.

2) Время блокирования больше 0 (блокирование новых сеансов связи).

Межсетевой экран блокирует новые сеансы связи на протяжении всего времени блокирования. Межсетевой экран удаляет самые старые существующие полуоткрытые сеансы связи, чтобы принять новые запросы на сеансы связи, когда истечет время блокирования.

Фильтрация трафика в ZyWALL

В ZyWALL определено три уровня фильтрации трафика:

1. Кадры Ethernet – необработанные кадры Ethernet

Правила создаются на основе сравнения определенного массива байт полученного кадра с определенной администратором маской такой же длины на основе побитового И.

2. Пакеты IP – собранные пакеты IP

Правила создаются на основе полей IP пакета (IP адресация, номер протокола, номер порта).

3. Правила Firewall

Конфигурирование правил фильтрации кадров Ethernet и пакетов IP возможно только через telnet и консоль.

Конфигурирование правил Firewall возможно только через Web.

Тема 2. Набор протоколов IPSec VPN в межсетевых экранах

Архитектура IPsec

Построение защищенного канала связи может быть реализовано на разных уровнях модели OSI.

Так, например, популярный SSL - протокол работает на уровне представления, а PPTP на канальном уровне.

В вопросе выбора уровня реализации защищенного канала несколько противоречивых аргументов: с одной стороны, за выбор верхних уровней говорит их независимость от вида транспортировки (выбора протокола сетевого и канального уровней), с другой стороны для каждого приложения необходима отдельная настройка и конфигурация.

Уровни OSI	**Протокол защищенного канала**
Прикладной уровень	S/MIME
Уровень представления	SSL, TLS
Сеансовый уровень	
Транспортный уровень	
Сетевой уровень	IPsec
Канальный уровень	PPTP
Физический уровень	

Плюсом в выборе нижних уровней является их универсальность и наглядность для приложений, минусом - зависимость от выбора конкретного протокола (например, PPP или Ethernet).

Компромиссом в выборе уровня является IPsec: он располагается на сетевом уровне, используя самый распространенный протокол этого уровня IP. Это делает IPsec более гибким, так что он может использоваться для защиты любых протоколов, базирующихся на TCP и UDP. В то же время, он прозрачен для большинства приложений.

IPsec является набором стандартов Интернет и своего рода «надстройкой» над IP-протоколом. Его ядро составляют три протокола:

1. Authentication Header (AH) обеспечивает целостность виртуального соединения (передаваемых данных), аутентификацию источника

информации и функцию по предотвращению повторной передачи пакетов,

2. Encapsulating Security Payload (ESP) обеспечивает конфиденциальность (шифрование) передаваемой информации, ограничение потока конфиденциального трафика. Кроме этого, он может исполнять функции AH: обеспечить целостность виртуального соединения (передаваемых данных), аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов. При применении ESP в обязательном порядке должен указываться набор услуг по обеспечению безопасности: каждая из его функций может включаться опционально,
3. Internet Security Association and Key Management Protocol (ISAKMP) — протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами. Протокол предусматривает использование различных механизмов обмена ключами, включая задание фиксированных ключей, использование таких протоколов, как Internet Key Exchange, Kerberized Internet Negotiation of Keys (RFC 4430) или записей DNS типа IPSECKEY (RFC 4025).

Также одним из ключевых понятий является Security Association (SA). По сути, SA является набором параметров, характеризующим соединение. Например, используемые алгоритм шифрования и хэш-функция, секретные ключи, номер пакета и др.

Туннельный и транспортный режимы

IPsec может функционировать в двух режимах: транспортном и туннельном. В транспортном режиме шифруются (или подписываются) только данные IP-пакета, исходный заголовок сохраняется.

Транспортный режим, как правило, используется для установления соединения между хостами. Он может также использоваться между шлюзами, для защиты туннелей, организованных каким-нибудь другим способом (см., например, L2TP).

В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовок, маршрутная информация, а затем он вставляется в поле данных нового пакета, то есть происходит инкапсуляция.

Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи (например, Интернет) между шлюзами для объединения разных частей виртуальной частной сети.

Режимы IPsec не являются взаимоисключающими. На одном и том же узле некоторые SA могут использовать транспортный режим, а другие - туннельный.

Security Association

Для начала обмена данными между двумя сторонами необходимо установить соединение, которое носит название SA (Security Association). Концепция SA фундаментальна для IPsec и описывает, как стороны будут использовать сервисы для обеспечения защищенного общения.

Соединение SA является симплексным (однонаправленным), поэтому для взаимодействия сторон необходимо установить два соединения. Стоит также отметить, что стандарты IPsec позволяют конечным точкам защищенного канала использовать одно SA для передачи трафика всех взаимодействующих через этот канал хостов, и создавать для этой цели произвольное число безопасных ассоциаций, например, по одной на каждое TCP-соединение. Это дает возможность выбирать нужную степень детализации защиты. OSI.

Установка соединения начинается с взаимной аутентификации сторон.

Далее происходит выбор параметров (будет ли осуществляться аутентификация, шифрование, проверка целостности данных) и необходимого протокола (AH или ESP) передачи данных.

После этого выбираются конкретные алгоритмы (например, шифрования, хэш-функция) из нескольких возможных схем, некоторые из которых определены стандартом (для шифрования DES, для хэш-функций MD5 либо SHA-1), другие добавляются производителями продуктов, использующих IPsec (например, Triple DES, Blowfish, CAST).

Security Associations Database

Все SA хранятся в базе данных SAD (Security Associations Database) IPsec-модуля. Каждое SA имеет уникальный маркер, состоящий из трех элементов:

- индекса параметров безопасности (Security Parameters Index, SPI),
- IP-адреса назначения,
- идентификатора протокола безопасности (ESP или AH).

IPsec-модуль, имея эти три параметра, может отыскать в SAD запись о конкретном SA. В список компонентов SA входят:

Последовательный номер -

32-битовое значение, которое используется для формирования поля *Sequence Number* в заголовках AH и ESP.

Переполнение счетчика порядкового номера -

Флаг, который сигнализирует о переполнении счетчика последовательного номера.

Окно для подавления атак воспроизведения -

Используется для определения повторной передачи пакетов. Если значение в поле *Sequence Number* не попадает в заданный диапазон, то пакет уничтожается.

Информация AH -

используемый алгоритм аутентификации, необходимые ключи, время жизни ключей и другие параметры.

Информация ESP -

алгоритмы шифрования и аутентификации, необходимые ключи, параметры инициализации (например, IV), время жизни ключей и другие параметры.

Режим работы IPsec -

туннельный или транспортный

Время жизни SA -

Задано в секундах или байтах информации, проходящих через туннель. Определяет длительность существования SA, при достижении этого значения текущее SA должно завершиться, при необходимости продолжить соединение, устанавливается новое SA.

MTU -

Максимальный размер пакета, который можно передать по виртуальному каналу без фрагментации.

Каждый протокол (ESP/AH) должен иметь свое собственное SA для каждого направления, таким образом, связка AH+ESP требует для дуплексного канала наличия четырех SA. Все эти данные располагаются в SAD.

В SAD содержатся:

- AH: алгоритм аутентификации,
- AH: секретный ключ для аутентификации,
- ESP: алгоритм шифрования,
- ESP: секретный ключ шифрования,
- ESP: использование аутентификации (да/нет),
- Параметры для обмена ключами,
- Ограничения маршрутизации,
- Политика IP-фильтрации.

Security Policy Database

Помимо базы данных SAD, реализации IPsec поддерживают базу данных SPD (Security Policy Database - база данных политики безопасности).

SPD служит для соотнесения приходящих IP-пакетов с правилами обработки для них. Записи в SPD состоя из двух полей.

В первом хранятся характерные признаки пакетов, по которым можно выделить тот или иной поток информации. Эти поля называются селекторами. Примеры селекторов, которые содержатся в SPD:

- IP-адрес места назначения,
- IP-адрес отправителя,
- Имя пользователя в формате DNS или X.500,
- Порты отправителя и получателя.

Второе поле в SPD содержит политику защиты, соответствующую данному потоку пакетов. Селекторы используются для фильтрации исходящих пакетов, с целью поставить каждый пакет в соответствие с определенным SA. Когда поступает пакет, сравниваются значения соответствующих полей в пакете (селекторные поля) с теми, которые содержатся в SPD. При нахождении совпадении в поле политики защиты содержится информация о том, как поступать с данным пакетом: передать без изменений, отбросить или обработать. В случае обработки, в этом же поле содержится ссылка на соответствующую запись в SAD. Затем определяется SA для пакета и сопряженный с ней индекс параметров безопасности(SPI). После чего выполняются операции IPsec(операции протокола AH или ESP). Если пакет входящий, то в нем сразу содержится SPI - проводится соответствующая обработка.

Authentication Header

Authentication Header format

Offsets	**Octet$_{16}$**	**0**								**1**								**2**								**3**			
Octet$_{16}$	**Bit$_{10}$**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	*Next Header*								*Payload Len*								*Reserved*													
4	**32**	*Security Parameters Index (SPI)*																													
8	**64**	*Sequence Number*																													
C	**96**	*Integrity Check Value (ICV)*																													
…	**…**	…																													

Тип следующего заголовка (8 bits) -

Тип заголовка протокола, идущего после заголовка AH. По этому полю приемный IP-sec модуль узнает о защищаемом протоколе верхнего уровня. Значения этого поля для разных протоколов можно посмотреть в RFC 1700.

Длина содержимого (8 bits) -

Это поле определяет общий размер AH-заголовка в 32-битовых словах, минус 2. Несмотря на это, при использовании IPv6 длина заголовка должна быть кратна 8 байтам.

Зарезервировано (16 bits) -

Зарезервировано. Заполняется нулями.

Индекс параметров системы безопасности (32 bits) -

Индекс параметров безопасности. Значение этого поля вместе с IP-адресом получателя и протоколом безопасности (AH-протокол), однозначно определяет защищенное виртуальное соединение(SA) для данного пакета. Диапазон значений SPI 1…255 зарезервирован IANA.

Порядковый номер(32 bits) -

Последовательный номер. Служит для защиты от повторной передачи. Поле содержит монотонно возрастающее значение параметра. Несмотря на то, что получатель может отказаться от услуги по защите от повторной передачи пакетов, оно является обязательным и всегда присутствует в AH-заголовке. Передающий IPsec-модуль всегда использует это поле, но получатель может его и не обрабатывать.

Данные для аутентификации -

Контрольная сумма. Служит для аутентификации и проверки целостности пакета. Должна быть кратна 8-байтам для IPv6, и 4-байтам для IPv4.

Протокол AH используется для аутентификации, то есть для подтверждения того, что мы связываемся именно с тем, с кем предполагаем, и что данные, которые мы получаем, не искажены при передаче.

Обработка выходных IP-пакетов

Если передающий IPsec-модуль определяет, что пакет связан с SA, которое предполагает AH-обработку, то он начинает обработку. В зависимости от режима (транспортный или режим туннелирования) он по-разному вставляет AH-заголовок в IP-пакет.

В транспортном режиме AH-заголовок располагается после заголовка протокола IP и перед заголовками протоколов верхнего уровня (Обычно, TCP или UDP).

В режиме туннелирования весь исходный IP-пакет обрамляется сначала заголовком AH, затем заголовком IP-протокола. Такой заголовок называется внешним, а заголовок исходного IP-пакета внутренним.

После этого передающий IPsec-модуль должен сгенерировать последовательный номер и записать его в поле Sequence Number.

При установлении SA последовательный номер устанавливается в 0, и перед отправкой каждого IPsec-пакета увеличивается на единицу.

Кроме того, происходит проверка: не зациклился ли счетчик. Если он достиг своего максимального значения, то он снова устанавливается в 0.

Если используется услуга по предотвращению повторной передачи, то при достижении счетчика своего максимального значения, передающий IPsec-модуль переустанавливает SA. Таким образом обеспечивается защита от повторной посылки пакета: приемный IPsec-модуль будет проверять поле Sequence Number, и игнорировать повторно приходящие пакеты.

Далее происходит вычисление контрольной суммы ICV. Надо заметить, что здесь контрольная сумма вычисляется с применением секретного ключа, без которого злоумышленник сможет заново вычислить хэш, но, не зная ключа, не сможет сформировать правильную контрольную сумму. Конкретные алгоритмы, использующиеся для вычисления ICV, можно

узнать из RFC 4305. В настоящее время могут применяться, например, алгоритмы HMAC-SHA1-96 или AES-XCBC-MAC-96. Протокол AH вычисляет контрольную сумму (ICV) по следующим полям IPsec-пакета:

- поля IP-заголовка, которые не были подвержены изменениям в процессе транслирования, или определены как наиболее важные,
- AH-заголовок (Поля: «Next Header», "Payload Len, «Reserved», «SPI», «Sequence Number», «Integrity Check Value». Поле «Integrity Check Value» устанавливается в 0 при вычислении ICV,
- данные протокола верхнего уровня.

Если поле может изменяться в процессе транспортировки, то его значение устанавливается в 0 перед вычислением ICV. Исключения составляют поля, которые могут изменяться, но значение, которых можно предугадать при приеме. При вычислении ICV они не заполняются нулями. Примером изменяемого поля может служить поле контрольной суммы, примером изменяемого, но предопределенного может являться IP-адрес получателя. Более подробное описание того, какие поля как учитываются при вычислении ICV, можно найти в стандарте RFC 2402.

Обработка входных IP-пакетов

После получения пакета, содержащего сообщение AH-протокола, приемный IPsec-модуль ищет соответствующее защищенное виртуальное соединение (SA) SAD (Security Associations Database), используя IP-адрес получателя, протокол безопасности (AH) и индекс SPI.

Если соответствующее соединение SA не найдено, пакет уничтожается. Найденное защищенное виртуальное соединение (SA) указывает на то, используется ли услуга по предотвращению повторной передачи пакетов, то есть на необходимость проверки поля Sequence Number.

Если услуга используется, то поле проверяется. При этом используется метод скользящего окна для ограничения буферной памяти, требуемый для работы протоколу.

Приемный IPsec-модуль формирует окно с шириной W (обычно W выбирается равным 32 или 64 пакетам). Левый край окна соответствует минимальному последовательному номеру (Sequence Number) N правильно принятого пакета. Пакет с полем Sequence Number, в котором содержится значение, начиная от N+1 и заканчивая N+W, принимается корректно. Если полученный пакет оказывается по левую границу окна, то он уничтожается.

Затем приемный IPsec-модуль вычисляет ICV по соответствующим полям принятого пакета, используя алгоритм аутентификации, который он узнает из записи об SA, и сравнивает полученный результат со значением ICV, расположенным в поле «Integrity Check Value».

Если вычисленное значение ICV совпало с принятым, то пришедший пакет считается действительным и принимается для IP-обработки. Если проверка дала отрицательный результат, то принятый пакет уничтожается.

Encapsulating Security Payload

Encapsulating Security Payload format

Offsets	**Octet $_{16}$**	**0**	**1**	**2**	**3**
Octet $_{16}$	**Bit $_{10}$**	**0 1 2 3 4 5 6 7 8 9**	**1 0 1 1 1 2 1 3 1 4 1 5 1 6 1 7 1 8 1 9**	**2 0 2 1 2 2 2 3 2 4 2 5 2 6 2 7 2 8 2 9**	**3 0 3 1**
0	**0**	*Security Parameters Index (SPI)*			
4	**32**	*Sequence Number*			
8	**64**	*Payload data*			
…	**…**				
…	**…**				
…	**…**	*Padding (0-255 octets)*			
…	**…**		*Pad Length*	*Next Header*	
…	**…**	*Integrity Check Value (ICV)*			
…	**…**	…			

Security Parameters Index (32 bits) -

Индекс параметров безопасности (аналогичен соответствующему полю AH). Значение этого поля вместе с IP-адресом получателя и протоколом безопасности(ESP-протокол), однозначно определяет защищенное виртуальное соединение(SA) для данного пакета. Диапазон значений SPI 1…255 зарезервирован IANA для последующего использования.

Sequence Number (32 bits) -

Последовательный номер(аналогичен соответствующему полю AH). Служит для защиты от повторной передачи. Поле содержит монотонно возрастающее значение параметра. Несмотря на то, что получатель может и отказаться от услуги по защите от повторной передачи пакетов, оно всегда присутствует в ESP-заголовке. Отправитель(передающий IPsec-модуль) должен всегда использовать это поле, но получатель может и не нуждаться в его обработке.

Payload data (variable) -

Содержит данные (в зависимости от выбора режима - туннельного или транспортного, здесь может находиться либо весь исходный инкапсулированный пакет, либо лишь его данные) в соответствии с полем «Next Header». Это поле является обязательным и состоит из целого числа байтов. Если алгоритм, который используется для

шифрования этого поля, требует данных для синхронизации криптопроцессов (например, вектор инициализации - «Initialization Vector»), то это поле может содержать эти данные в явном виде.

Padding (0-255 octets) -

Дополнение. Необходимо, например, для алгоритмов, которые требуют, чтобы открытый текст был кратен некоторому числу байтов), например, размеру блока для блочного шифра.

Pad Length (8 bits) -

Размер дополнения(в байтах).

Next Header (8 bits) -

Это поле определяет тип данных, содержащихся в поле «Payload data».

Integrity Check Value -

Контрольная сумма. Служит для аутентификации и проверки целостности пакета. Должна быть кратна 8-байтам для IPv6, и 4-байтам для IPv4.

Обработка выходных IPsec-пакетов

Если передающий IPsec-модуль определяет, что пакет связан с SA, которое предполагает ESP-обработку, то он начинает обработку. В зависимости от режима (транспортный или режим туннелирования) исходный IP-пакет обрабатывается по-разному.

В **транспортном** режиме передающий IPsec-модуль осуществляет процедуру обрамления протокола верхнего уровня (например, TCP или UDP), используя для этого ESP-заголовок (поля Security Parameters Index и Sequence Number заголовка) и ESP-концевик (остальные поля заголовка, следующие за полем данных - Payload data), не затрагивая при этом заголовок исходного IP-пакета.

В режиме **туннелирования** IP-пакет обрамляется ESP-заголовком и ESP-концевиком (инкапсуляция), после чего обрамляется внешним IP-заголовком (который может не совпадать с исходным, например, если IPsec модуль установлен на шлюзе).

Далее производится шифрование: в транспортном режиме шифруется только сообщение протокола вышележащего уровня (то есть все, что находилось после IP-заголовка в исходном пакете), в режиме туннелирования шифруется весь исходный IP-пакет.

Передающий IPsec-модуль из записи о SA определяет алгоритм шифрования и секретный ключ. Стандарты IPsec разрешают использование алгоритмов шифрования Triple DES, AES и Blowfish, если их поддерживают обе стороны. Иначе используется DES, описанный в RFC 2405. Так как размер открытого текста должен быть кратен определенному числу байт, например, размеру блока для блочных

алгоритмов, перед шифрованием производится еще и необходимое дополнение шифруемого сообщения.
Защифрованное сообщение помещается в поле Payload Data. В поле Pad Length помещается длина дополнения. Затем, как и в AH, вычисляется Sequence Number.
После чего рассчитывается контрольная сумма (ICV). Контрольная сумма, в отличие от протокола AH, где при ее вычислении учитываются также и некоторые поля IP-заголовка, в ESP вычисляется только по полям ESP-пакета за вычетом поля ICV. Перед вычислением контрольной суммы оно заполняется нулями. Алгоритм вычисления ICV, как и в протоколе AH, передающий IPsec-модуль узнает из записи об SA, с которым связан обрабатываемый пакет.

Обработка входных IPsec-пакетов

После получения пакета, содержащего сообщение ESP-протокола, приемный IPsec-модуль ищет соответствующее защищенное виртуальное соединение(SA) в SAD, используя IP-адрес получателя, протокол безопасности (ESP) и индекс SPI.
Если соответствующее соединение SA не найдено, пакет уничтожается. Найденное защищенное виртуальное соединение (SA) указывает на то, используется ли услуга по предотвращению повторной передачи пакетов, то есть на необходимость проверки поля Sequence Number.
Если услуга используется, то поле проверяется. Для этого, так же как и в AH, используется метод скользящего окна. Приемный IPsec-модуль формирует окно с шириной W. Левый край окна соответствует минимальному последовательному номеру (Sequence Number) N правильно принятого пакета. Пакет с полем Sequence Number, в котором содержится значение, начиная от N+1 и заканчивая N+W, принимается корректно. Если полученный пакет оказывается по левую границу окна - он уничтожается.
Затем, если используется услуга аутентификации, приемный IPsec-модуль вычисляет ICV по соответствующим полям принятого пакета, используя алгоритм аутентификации, который он узнает из записи об SA, и сравнивает полученный результат со значением ICV, расположенным в поле «Integrity Check Value».
Если вычисленное значение ICV совпало с принятым, то пришедший пакет считается действительным.
Если вычисленное значение ICV не совпало с принятым, то пришедший пакет уничтожается.
Далее производится расшифровывание пакета. Приемный IPsec-модуль узнает из записи об SA, какой алгоритм шифрования используется и секретный ключ.

Проверка контрольной суммы и процедура расшифровывания могут проводиться не только последовательно, но и параллельно. В последнем случае процедура проверки контрольной суммы должна закончиться раньше процедуры расшифровывания, и если проверка ICV провалилась, процедура расшифровывания также должна прекратиться. Это позволяет быстрее выявлять испорченные пакеты, что, в свою очередь, повышает уровень защиты от атак типа «отказ в обслуживании» (DOS-атаки). Далее расшифрованное сообщение в соответствии с полем Next Header передается для дальнейшей обработки.

IKE

IKE (Internet Key Exchange) - протокол, который обеспечивает первоначальную аутентификацию сторон, а также их обмен общими секретными ключами. Процесс работы IKE протокола можно разбить на две фазы.

Первая фаза IKE

IKE создает безопасный канал между двумя узлами, называемый IKE security association (IKE SA). Также, в этой фазе два узла согласуют сессионный ключ по алгоритму Диффи-Хеллмана. Первая фаза IKE может проходить в одном из двух режимов:

1. Основной режим, который состоит из трех двусторонних обменов между отправителем и получателем:
    - Во время первого обмена согласуются алгоритмы и хэш-функции, которые будут использоваться для защиты IKE соединения, посредством сопоставления IKE SA каждого узла,
    - Используя алгоритм Диффи-Хеллмана, стороны обмениваются общим секретным ключом. Также узлы проверяют идентификацию друг друга путем передачи и подтверждения последовательности псевдослучайных чисел,
    - По зашифрованному IP-адресу проверяется идентичность противоположной стороны. В результате выполнения основного режима создается безопасный канал для последующего ISAKMP — обмена (этот протокол определяет порядок действий для аутентификации соединения узлов, создания и управления SA, генерации ключей, а также уменьшения угроз, таких как DoS-атака или атака повторного воспроизведения).
2. Агрессивный режим

Этот режим производится меньшим числом обменов и, соответственно, числом пакетов. В первом сообщении помещается практически вся нужная для установления IKE SA информация: открытый ключ Диффи-Хеллмана, для синхронизации пакетов, подтверждаемый другим участником, идентификатор пакета. Получатель посылает в ответ все, что надо для завершения обмена. Первому узлу требуется только подтвердить соединение. С точки зрения безопасности агрессивный режим является слабым, так как участники начинают обмениваться информацией до установления безопасного канала, поэтому возможен несанкционированный перехват данных. Однако, агрессивный режим работает быстрее, чем основной.

Вторая фаза IKE

В фазе два IKE существует только быстрый режим.
Быстрый режим выполняется только после создания безопасного канала в ходе первой фазы. Он согласуют общую политику IPsec, получает общие секретные ключи для алгоритмов протоколов IPsec (AH или ESP), устанавливает IPsec SA. Использование последовательных номеров обеспечивает защиту от атак повторной передачи.
Также быстрый режим используется для пересмотра текущей IPsec SA и выбора новой, когда время жизни SA истекает. Обычно быстрый режим проводит обновление общих секретных ключей, используя алгоритм Диффи-Хеллмана из первой фазы.

Работа протоколов IPsec

В работе протоколов IPsec можно выделить пять этапов:

1. первый этап начинается с создания на каждом узле, поддерживающем стандарт IPsec, политики безопасности. На этом этапе определяется, какой трафик подлежит шифрованию, какие функции и алгоритмы могут быть использованы.
2. второй этап является первой фазой IKE. Ее цель: организовать безопасный канал между сторонами для второй фазы IKE. На втором этапе выполняются:
   - Аутентификация и защита идентификационной информации узлов,
   - Проверка соответствий политик IKE SA узлов для безопасного обмена ключами,
   - Обмен Диффи-Хеллмана, в результате которого у каждого узла будет общий секретный ключ,
   - Создание безопасного канала для второй фазы IKE.
3. третий этап является второй фазой IKE. Его задачей является создание IPsec туннеля. На третьем этапе выполняются следующие функции:

- Согласуются параметры IPsec SA по защищаемому IKE SA каналу, созданному в первой фазе IKE,
- Устанавливается IPsec SA,
- Периодически осуществляется пересмотр IPsec SA, чтобы убедиться в ее безопасности,
- (Опционально) выполняется дополнительный обмен Диффи-Хеллмана.

4. рабочий этап. После создания IPsec SA начинается обмен информацией между узлами через IPsec-туннель, используются протоколы и параметры, установленные в SA,
5. прекращают действовать текущие IPsec SA. Это происходит при их удалении или при истечении времени жизни (определенное в SA в байтах информации, передаваемой через канал, или в секундах), значение которого содержится в SAD на каждом узле. Если требуется продолжить передачу, запускается фаза два IKE (если требуется, то и первая фаза) и далее создаются новые IPsec SA. Процесс создания новых SA может происходить и до завершения действия текущих, если требуется непрерывная передача данных.

Использование IPsec

Протокол IPsec используется, в основном, для организации VPN-туннелей. В этом случае протоколы ESP и AH работают в режиме туннелирования.

Кроме того, настраивая политики безопасности определенным образом, протокол можно использовать для создания межсетевого экрана.

Смысл межсетевого экрана заключается в том, что он контролирует и фильтрует проходящие через него пакеты в соответствии с заданными правилами.

Устанавливается набор правил, и экран просматривает все проходящие через него пакеты. Если передаваемые пакеты попадают под действие этих правил, межсетевой экран обрабатывает их соответствующим образом. Например, он может отклонять определенные пакеты, прекращая небезопасные соединения.

Настроив политику безопасности соответствующим образом, можно, например, запретить веб-трафик. Для этого достаточно запретить отсылку пакетов, в которые вкладываются сообщения протоколов HTTP и HTTPS.

IPsec можно применять и для защиты серверов - для этого отбрасываются все пакеты, кроме пакетов, необходимых для корректного выполнения функций сервера. Например, для Web-сервера можно блокировать весь трафик, за исключением соединений через 80-й порт протокола TCP, или через порт TCP 443 в случаях, когда применяется HTTPS. С помощью IPsec здесь обеспечивается безопасный доступ пользователей к серверу. При использовании протокола ESP, все обращения к серверу и его ответы

шифруются. Однако за VPN-шлюзом (в домене шифрования) передаются открытые сообщения.
Другие примеры использования IPsec:

- шифрование трафика между файловым сервером и компьютерами в локальной сети, используя IPsec в транспортном режиме,
- соединение двух офисов с использованием IPsec в туннельном режиме.

Тема 3. IPSec VPN в межсетевых экранах ZyWALL

При помощи набора IPSec протоколов можно реализовать защиту передаваемых данных и аутентификацию на базе следующих услуг:

- аутентификация,
- целостность данных,
- шифрование,
- защита от повторной передачи.

PPTP (Point-to-Point Tunneling Protocol) - протокол туннелирования "точка-точка". PPTP создан компаниями Microsoft, US Robotics и другими. Этот протокол туннелирования был разработан советом PPTP и позволяет инкапсулировать пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и Интернет).
PPTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу предприятия путем создания в сети TCP/IP частной виртуальной сети.
L2TP (Layer 2 Tunneling Protocol, протокол туннелирования уровня 2). Объединение протоколов L2F и PPTP, произведенное компаниями Cisco Systems по рекомендации IEFT(Internet Engineering Task Force).
Наиболее распространенным протоколом VPN в настоящее время является IPSec. Более 65 процентов частных виртуальных сетей создано на его основе.
При помощи IPSec можно реализовать защиту передаваемых данных и аутентификацию отправителя на базе следующих услуг:

- **Аутентификация** - при использовании IPSec получатель сообщения может верифицировать источник полученных пакетов и удостовериться в целостности данных,
- **Целостность** - при использовании IPSec получатель может проверить целостность пакетов данных, переданных отправителем, чтобы убедиться в том, что данные не были изменены в процессе передачи,
- **Защита от повторной передачи** - необходимость 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,

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

Например, 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.

Топология VPN IPSec

Чтобы сконфигурировать соединение ZyWALL VPN, необходимо знать подробную информацию о соединении по протоколу IPSec. Эта информация о соединении содержит:

1. **IP-адрес** - IP-адреса устройств, которые хотят установить VPN-соединение, включая шлюз безопасности и хосты,
2. **Протокол обеспечения безопасности** - протокол, который предполагается использовать (AH или ESP),
3. **Метод управления ключами** - метод поддержания соединения SA между системами,
4. **Алгоритм шифрования** - выбрать алгоритм шифрования,
5. **Алгоритм аутентификации** - выбрать алгоритм аутентификации,
6. **Ключевая группа** - выбрать ключевую группу для реализации криптографического метода Диффи-Хеллмана (с открытыми ключами),
7. **Режим инкапсуляции** - выбрать туннельный или транспортный режим.

Хеш-функции

Хеш-функция - это математическая функция, которая позволяет преобразовывать входную последовательность данных произвольной длины в строку фиксированной длины. Результат работы хеш-функции называют хешем, хеш-кодом или дайджестом сообщения. Хэш-функция обладает следующими свойствами:

- невозможно получить исходную последовательность данных из хеш-кода,
- практически невозможно найти два различных исходных массива, которые бы обращались в один и тот же хэш-код.

Существует большое число различных хеш-функций, в оборудовании ZyXEL
используются следующие:

- MD5
- SHA1

Различия хеш-функций MD5 и SHA-1:

- длина хеш-кода функции MD5 — 16 байт,
- длина хещ-кода функции SHA-1 — 20 байт,
- SHA-1 работает приблизительно на 25% медленнее MD5 (на той же аппаратуре), однако ключ SHA-1 длиннее на 4 байта, а, следовательно, гораздо труднее создать два различных сообщения, имеющие одинаковый хеш-код.

Пример работы хеш-функции MD5

Например, для работы хеш-функции MD5 имеем два исходных файла:

- 1.txt, который содержит текст «1234567890»,
- 2.txt, который содержит текст «1234567891».

Отметим, что исходные файлы различаются лишь 1 символом.

Далее рассчитаем хеш-код по каждому из файлов и видим, что, несмотря на то, что исходная последовательность отличается лишь 1 символом, хеш-коды отличаются кардинально:

MD5(1.txt) = 7ff7ad3ae5bebc01f77234a7949846c2 ,

MD5(2.txt) = 0c8dd2203e38e6c16e94469e80dbf43c .

Аутентификация, целостность данных

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

Хэш-код полученный в результате работы функции HMAC называют MAC (Message Authentication Code).

Использование функции HMAC позволяет не только аутентифицировать отправителя, но и обеспечить целостность данных.

Например, если сообщение, требующее аутентификации перехватить по пути следования и модифицировать его, то MAC, вычисленный получателем не будет совпадать с MAC пришедшим, так как сообщение было изменено. Перехватить сообщение, модифицировать его и изменить MAC тоже невозможно, так как неизвестен секретный ключ.

Защита от повторной передачи

Отправитель в каждом пакете заполняет поле «порядковый номер» и, начиная с первого пакета, это поле увеличивается на 1.

В случае если кто-то перехватывает пакет по пути следования и совершает повторную передачу, то получатель данный пакет отбросит, т.к. обнаружит дублирование порядковых номеров.

Шифрование

Шифрова́ние – это способ преобразования данных из одного представления в другое - из *«открытого»* представления в *«закрытое»*. Под *«открытым»* представлением понимаются данные, содержащие информацию в том виде, в котором она существует (например, обычный текст). Под *«закрытым»* - видоизмененные данные, которые не содержат изначальной информации. Для того чтобы прочитать изначальную информацию, необходим ключ и дешифратор (специальное устройство или программа). То есть злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не сможет прочитать из них передаваемую информацию.

Существует два типа алгоритмов шифрования:

- симметричный - такой тип шифрования, при котором для шифровки и дешифровки используется один и тот же ключ.
- асимметричный - такой тип шифрования, при котором для шифровки и дешифровки используются разные ключи.

К симметричным алгоритмам относятся DES, 3DES и AES, к асимметричным относятся RSA, DSA.

Асимметричный алгоритм шифрования работает на два-три порядка медленнее, чем симметричный, однако его можно использовать не только для шифрования и дешифровки текста, но и для создания электронно-цифровой подписи.

Симметричные алгоритмы шифрования используются в устройствах ZyWALL USG для шифрования сообщения, так как они обеспечивают большую криптостойкость при равных вычислительных затратах.

Асимметричные алгоритмы шифрования в устройствах ZyWALL USG применяются для создания электронно-цифровой подписи, то есть для аутентификации удаленной стороны.

IPSec VPN алгоритм обмена ключами

Алгоритм Диффи-Хеллмана 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).

Группы Диффи-Хеллмана

Группы Диффи-Хеллмана – это пары значений p и g, описанные в стандарте RFC 2409 и RFC 3526. В практических реализациях чаще всего значение p и g не передаются от отправителя получателю. Вместо этого отправляющая и принимающая стороны имеет предварительно согласованные группы Диффи-Хеллмана, которые представляют собой пару значений p и g. Определено больше число групп Диффи-Хеллмана, в

оборудовании ZyXEL поддерживаются следующие группы DH 1, DH 2, DH 5.

DH1

p = 2^768 - 2 ^704 - 1 + 2^64 * { [2^638 *pi*] + 149686 }

g = 2

DH2

p = 2^1024 - 2^960 - 1 + 2^64 * { [2^894 *pi*] + 129093 }

g = 2

DH5

p = 2^1536 - 2^1472 - 1 + 2^64 * { [2^1406 *pi*] + 741804 }

g = 2

Чем больше номер группы Диффи-Хеллмана, тем выше криптостойкость.

При работе алгоритма Диффи-Хеллмана DH (Diffie-Hellman), каждая сторона выполняет следующие действия:

1. генерирует случайное натуральное число a - *закрытый ключ*
2. совместно с удалённой стороной устанавливает *открытые параметры* p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где:

   p является случайным простым числом

   g является первообразным корнем по модулю p
3. вычисляет *открытый ключ* A, используя преобразование над *закрытым ключом:*

   $A = g^a \bmod p$
4. обменивается *открытыми ключами* с удалённой стороной
5. вычисляет *общий секретный ключ* K, используя открытый ключ удаленной стороны B и свой закрытый ключ a*:*

   $K = B^a \bmod p$

K получается равным с обеих сторон, потому что:

$B^a \bmod p = (g^b \bmod p)^a \bmod p = \boldsymbol{g^{ab} \bmod p} = (g^a \bmod p)^b \bmod p = A^b \bmod p$

В практических реализациях, для a и b используются числа порядка 10^{100} и p порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

Криптографическая стойкость

Криптографическая стойкость алгоритма Диффи - Хеллмана (сложность вычисления $K=g^{ab} \bmod p$ по известным p, g, $A=g^a \bmod p$ и $B=g^b \bmod p$) основана на предполагаемой сложности проблемы дискретного логарифмирования.

Хотя умение решать проблему дискретного логарифмирования позволит взломать алгоритм Диффи - Хеллмана, обратное утверждение до сих пор является открытым вопросом (другими словами, эквивалентность этих проблем не доказана).

Алгоритм Диффи - Хеллмана работает только на линиях связи, надёжно защищённых от модификации. Если бы он был применим на любых открытых каналах, то давно снял бы проблему распространения ключей и, возможно, заменил собой всю асимметричную криптографию.
Однако, в тех случаях, когда в канале возможна модификация данных, появляется возможность атаки «человек посередине». Атакующий заменяет сообщения переговоров о ключе на свои собственные и получает два ключа - свой для каждого из законных участников протокола. Далее атакующий может перешифровать переписку между участниками своим ключом для каждого из законных участников протокола, и ознакомиться с их сообщениями, оставаясь незамеченным.

IPSec VPN. Системы криптографии с открытым ключом

Криптографическая система с **отрытым ключом** (**ассиметричное** шифрование) - это система шифрования и/или электронной подписи, при которой открытый ключ передается по отрытому незащищенному доступному для наблюдения каналу и используется для проверки электронной цифровой подписи (ЭЦП) и для шифровки сообщения.
Для генерации ЭЦП и для дешифровки сообщения используется секретный ключ.
ЭЦП обеспечивает аутентификацию, так как, не зная секретного колюча отправителя, невозможно создать цифровую подпись, которая бы верного проверялась с помощью открытого ключа отправителя.
ЭЦП обеспечивает также целостность данных (т.к. если попытаться изменить сообщение в процессе передачи, то не будет возможности составить корректную цифровую подпись, не имея секретного ключа отправителя).
ЭЦП – это реквизит электронного документа, предназначенный для защиты от подделки, полученный в результате криптографического преобразования с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца подписи, а также установить отсутствие искажения информации в электронном документе.
Уязвимость заключатся в выяснении подлинности третьей стороны, которая решается с помощью центров сертификации и сертификатов.

IPSec VPN Сертификаты

В криптографии центр сертификации или удостоверяющий центр (англ. Certification authority, CA) – это сторона, отдел, организация, чья честность неоспорима, а открытый ключ широко известен.
Задача центра сертификации: подтверждать подлинность ключей шифрования с помощью сертификатов электронной подписи.
Технически центр сертификации реализован как компонент глобальной службы каталогов, отвечающий за управление криптографическими

ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Центр сертификации - это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов, имеющих следующую структуру:

- серийный номер сертификата,
- объектный идентификатор алгоритма электронной подписи,
- имя удостоверяющего центра,
- срок действия сертификата,
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат),
- открытые ключи владельца сертификата (ключей может быть несколько),
- объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата,
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хеширования всей информации, хранящейся в сертификате).

Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем самоподписанного сертификата в списке удостоверенных корневых сертификатов. Корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом, аккредитованный центр получает «техническое право» работы и наследует «доверие» от организации, выполнившей аккредитацию.

Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией, проводящей аккредитацию в своих интересах и в соответствии со своими правилами.

Порядок аккредитации и требования, которым должен отвечать аккредитованный центр сертификации ключей, устанавливаются соответствующим уполномоченным органом государства или организации, выполняющей аккредитацию.

Центр сертификации ключей имеет право:

- предоставлять услуги по удостоверению сертификатов электронной цифровой подписи,
- обслуживать сертификаты открытых ключей,

- получать и проверять информацию, необходимую для создания соответствия информации указанной в сертификате ключа и предъявленными документами.

IPSec VPN протоколы

Протоколы IPSec работают на сетевом уровне (уровень 3 модели OSI). IPSec-протоколы можно разделить на два класса:

- протоколы, отвечающие за защиту потока передаваемых пакетов,
- протоколы согласования ассоциаций защиты.

В настоящее время определёны следующие протоколы IPSec:

- протокол согласования ассоциаций защиты - **IKE** (Internet Key Exchange), который работает на базе протокола ISAKMP (Internet Security Association and Key Management Protocol),
- протоколы, обеспечивающие 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, представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон. Составляющими такой политики может алгоритм шифрования, алгоритм аутентификации и т.д.

IPSec VPN IKE

Для того чтобы VPN выполняла функцию защиты данных, необходимо осуществить процесс согласования параметров **IKE** состоящий из **стадии 1 и стадии 2)**.

После согласования на **стадии 1** генерируются параметры безопасности, включая алгоритмы шифрования/аутентификации и ключи.

Эти параметры, используемые для защиты данных, носят название **безопасного туннеля**.

Согласование параметров на **стадии 2** протекает под защитой этого туннеля.

После согласования на стадии 2 генерируется второй набор параметров безопасности. Эти параметры используются для создания другого безопасного туннеля. Этот второй туннель и используется VPN для передачи данных. Шифрование и аутентификация данных выполняются в соответствии с параметрами безопасности, согласованными на стадии 2.

Для согласования параметров IKE на стадиях 1 и 2 используется протокол UDP с номером протокола 17 и портом 500. А для передачи данных

используется ESP или AH (номер протокола 50 или 51). Для ESP и AH номер порта не нужен.

IKE стадия 1

Аутентификация на первой стадии может производиться на базе предварительно согласованного ключа и на базе сертификатов. Производимый обмен данными зависит от метода аутентификации. Результатом работы стадии 1 станет появление безопасного соединения, внутри которого можно согласовывать параметры ESP/AH.

IKE стадия 2

На второй стадии согласуются протокол защиты, алгоритм шифрования и аутентификации, режим работы туннельный/транспортный и группа Диффи-Хеллмана при включенной функции PFS.

PFS (Perfect Forward Secrecy) - функция, позволяющая произвести дополнительный обмен по алгоритму Диффи-Хеллмана на второй стадии IKE, 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.

Тема 4. IPSec VPN режимы межсетевых экранов ZyWALL

Транспортный режим обеспечивает безопасное соединение двух узлов путем инкапсуляции тела IP-пакета в пакет AH либо ESP.

Туннельный режим обеспечивает безопасное соединение двух узлов путем инкапсуляции всего IP-пакета весь IP-пакет в AH либо ESP. Чаще всего используется именно туннельный режим.

Протоколы защиты

Как уже было сказано, существует две типа протоколов IPSec, обеспечивающих защиту потока передаваемых пакетов:

- ESP (Encapsulation Security Payload, инкапсуляция зашифрованных данных),
- 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.

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.

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**.
Использование протокола AH в транспортном режиме применяется для защиты виртуальных соединений типа «точка-точка», и чаще всего получается, что рабочая станция есть клиент IPSec. В транспортном режиме пакет модифицируется добавлением заголовка AH между заголовком IP и телом IP-пакета.

AH в транспортном режиме

Так как IP заголовок тоже аутентифицируется, то протокол AH не совместим с NAT, поскольку NAT изменяет поля адреса источника. Это означает, что хеш-код, который вычислит принимающая сторона не совпадет с хеш-кодом, передаваемом в заголовке AH. Данное замечание справедливо для транспортного и для туннельного режима.

AH в туннельном режиме

Туннельный режим обычно применяют между шлюзами для построения виртуальной локальной сети или между рабочей станцией и шлюзом для обеспечения безопасного доступа в локальную сеть за шлюзом.

ESP в транспортном режиме

Протокол ESP позволяет не только аутентифицировать источник данных, но и обеспечивать конфиденциальность (шифрование) данных. Использование протокола ESP в транспортном режиме применяется для защиты виртуальных соединений точка-точка, т.е. чаще всего получается, что рабочая станция и есть клиент IPSec.

ESP в туннельном режиме

В туннельном режиме весь пакет IP инкапсулируется в ESP пакет и в таком виде доставляется адресату. Протокол ESP и NAT способны работать вместе до тех пор, пока NAT подменяет только адреса. Если присутствует реализация NAPT (network address port translation), то есть подменяются IP-адреса и порты TCP/IP, то необходимо использовать дополнительную функцию NAT Traversal

NAT Traversal

NAT (от англ. *Network Address Translation* - «преобразование сетевых адресов») - это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия *IP Masquerading*, *Network Masquerading* и *Native Address Translation*.

Принцип работы функции NAT Traversal заключается в том, что между ESP заголовком и IP заголовком помещается заголовок UDP.
Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством - маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, который состоит в замене адреса источника (англ. *source*) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. *destination*) в ответном пакете.
Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.
Принимая пакет от локального компьютера, роутер анализирует IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в Интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из Интернета будет недоступен. Поэтому роутер «на лету» производит трансляцию IP-адреса и порта, и запоминает эту трансляцию у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер удалит из таблицы запись о *n*-ом порте за сроком давности.
Помимо *source* NAT (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также *destination* NAT (DNAT), когда обращения извне транслируются межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).
Существует 3 базовых концепции трансляции адресов:

- статическая (Static Network Address Translation),
- динамическая (Dynamic Address Translation),
- маскарадная (NAPT, NAT Overload, PAT).

Статический NAT - отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес (один к одному). Статический NAT полезен, когда устройство должно быть доступным снаружи сети.
Динамический NAT - отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.
Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) - форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети

транслируется в тот же самый адрес, но с различным номером порта. Механизм NAT определён в RFC 1631, RFC 3022.

NAT выполняет три важных функции:

1. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), 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 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами,
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 (а она может быть созданной при инициации соединения или статической), 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 (или форум) для осведомлённых посетителей можно будет попасть по адресу http://example.org:54055, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и скрытие «непубличных» ресурсов.

Недостатки NAT следующие:

1. 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 командах протокола FTP),
2. Из-за трансляции адресов «многие к одному» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные журналы трансляций,
3. DoS со стороны узла, осуществляющего NAT - если NAT используется для подключения многих пользователей к одному и

тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений. Частичным решением проблемы является использование пула адресов (группы адресов), для которых осуществляется трансляция,

4. В некоторых случаях, необходимость в дополнительной настройке (см. Трансляция порт-адрес) при работе с пиринговыми сетями и некоторыми другими программами, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие. Однако, если NAT-устройство и ПО, требующее дополнительной настройки, поддерживают технологию Universal Plug & Play, то в этом случае настройка произойдет полностью автоматически и прозрачно для пользователя.

NAT Traversal (прохождение или автонастройка NAT) - это набор возможностей, позволяющих сетевым приложениям определять, что они находятся за устройством, обеспечивающим NAT, узнавать внешний IP-адрес этого устройства и выполнять сопоставление портов для пересылки пакетов из внешнего порта NAT на внутренний порт, используемый приложением.

Это выполняется автоматически, пользователю нет необходимости вручную настраивать сопоставления портов или вносить изменения в какие-либо другие параметры.

Однако необходимы меры предосторожности при доверии к таким приложениям, т.к. они получают обширный контроль над устройством. Появляются потенциальные уязвимости.

IPSec VPN Site-to-Site

Наиболее часто используемый режим VPN - это Site-to-Site, схема, в которой безопасное соединение организуется между двумя сетями.

Чтобы создать Site-to-Site VPN необходимо на обеих сторонах туннеля настроить параметры первой и второй фазы.

Протокол IKE явно не определяет, как известить клиентскую сторону, если одна сторона туннеля изменила адрес или перезапустила систему. Следовательно, клиентская сторона будет сохранять зомби-туннель. Зомби-туннель будет мешать созданию нового туннеля даже с динамической или перезапускаемой стороны.

Dead Peer Detection

Dead Peer Detection (DPD) - механизм, с помощью которого ZyWALL может проверить работоспособность удаленного шлюза безопасности.

Алгоритм работы функции DPD следующий:

1. ZyWALL получает пакет, который необходимо отправить в VPN туннель,
2. В случае, если в течение последних 15 секунд по этому туннелю передавался трафик, то пакет будет отправлен,
3. В случае, если в течение последних 15 секунд по этому туннелю трафик не передавался, то ZyWALL отправит удаленному узлу HELLO пакет,
4. Удаленная сторона на полученный HELLO пакет отвечает ACK пакетом, тем самым, подтверждая свою работоспособность,
5. В случае, если удаленная сторона не ответила ACK пакетом, ZyWALL разрывает туннель и пытается установить его заново.

Проверки доступности туннеля

В ZyWALL реализованы несколько алгоритмов проверки доступности туннеля. Когда VPN-туннель установлен, ZyWALL будет использовать таймер простоя для входящего или исходящего трафика, в зависимости от используемого типа таймера. Если время простоя закончилось, то ZyWALL либо будет использовать алгоритм DPD, либо уничтожит SA на Стадии 1 и на Стадии 2, что разорвет VPN-туннель.

При алгоритме Dead Peer Detection (DPD) происходит следующее:

- и инициатор, и ответчик могут посылать HELLO пакеты
- получатель должен ответить ACK пакетом
- если ответные ACK пакеты не получены 5 раз, то туннель сбрасывается

После определенного времени с момента последнего получения данных от удаленной стороны, ZyWALL необходимо удостовериться, что удаленная сторона работоспособна при помощи HELLO пакетов.

При получении пакетов IPSec нет необходимости в отправке DPD пакетов.

Если одна сторона отправляет данные, и нет входящих пакетов в течение определенного времени, то необходимо установить таймер простоя и использовать HELLO пакеты.

Настройка таймера простоя для DPD

Для работы DPD необходимо определить время простоя туннеля после последней передачи данных. Это возможно сделать в меню VPN на закладке Global Settings:

- Output Idle Timer определяет время простоя туннеля после последней отправки данных,
- Input Idle Timer определяет время простоя туннеля после последнего получения данных,

– Gateway Domain Name Update Timer определяет время жизни разрешения DNS-IP удаленного шлюза безопасности, если он задан DNS именем.

Поддержка постоянного соединения

Имеется возможность поддержки постоянного соединения с помощью функции VPN Nail-Up. При этом туннель всегда «поднят»: при перезагрузке системы, после того как истекло время SA, после ручного разрыва соединения. Для поддержки постоянного соединения WAN nail-up должен быть активирован. Функция WAN nail-up позволяет поддерживать постоянное соединение с Internet.

Например, что произойдет, если пользователь сконфигурирует правило VPN nail up, но не включит WAN nail up? Это вызовет проблемы. Например, ZyWALL использует адрес 211.72.100.100 в качестве WAN IP-адреса при установке туннеля. Через какое-то время таймер простоя WAN соединения истекает, что приведет к разрыву VPN туннеля.

ZyWALL заново установит VPN туннель, на что потребуется какое-то время, что приведет к потере пакетов. Возможно изменение IP-адреса и возникновение «зомби»-туннеля с другой стороны.

Динамические правила VPN туннелей НЕ поддерживают Nail up.

С точки зрения ответчика адрес инициатора не известен до получения IKE пакета на установление туннеля. Это и не позволяет включить функцию nail up на ответной стороне.

Для инициатора возможно включение nail up, но это вызовет другие проблемы. Т.к. это динамическое правило, IP-адрес может меняться время от времени. Каждый раз при смене IP-адреса инициатор должен разрывать туннель. Функция “nail up” включена, что приведет к попытке установить туннель заново с новым IP-адресом.

Но в этот момент старый туннель все еще работает на отвечающей стороне, т.к. не было получено DEL пакета от инициатора. Это приведет к появлению «зомби»-туннеля, который может быть разорван по DPD алгоритму.

Необходимо включить функцию «**Check IPSec Tunnel connectivity**» на стадии 2. В этом случае, после установления фазы 1 ZyWALL делает предположение, что произошел сбой на удаленной стороне в связи со сменой IP-адреса. Таким образом, новое соединение будет установлено вместо старого. При помощи этой функции можно поддерживать nail-up для динамических правил со стороны ответной стороны.

IPSec VPN Site-to-Site with Dynamic Peer

Site-to-Site with Dynamic Peer может быть установлен только со стороны, которая имеет динамический IP-адрес. При этом политики маршрутизации настраиваются как обычно.

Динамический адрес с двух сторон туннеля

Если на обеих сторонах туннеля используются динамические адреса, то необходимо воспользоваться дополнительной функцией DynDNS, которая сопоставляет постоянное доменное имя динамическому IP-адресу.

IPSec VPN Remote Access

Удаленный доступ IPSec VPN возможен двух видов: в роли сервера и в роли клиента.

1. Remote Access (Server Role)

Remote Access (Server Role) используется для подключения конечного клиента, политики маршрутизации будут созданы автоматически. Для детальной настройки необходимо отметить пункт Use Policy Route to control dynamic IPSec rules.

2. Remote Access (Client Role)

Remote Access (Client Role) используется для подключения ZyWALL как конечного клиента, т.е. на удаленной стороне должен находится ZyWALL, работающий в режиме Remote Access (Server Role).

Тема 5. Использование SNAT и DNAT межсетевыми экранами ZyWALL

Архитектура передачи и проверки трафика устройством ZyWALL USG производится, используя следующие аббревиатуры.

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, предназначенных 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

Входящий трафик превращается в проверенный трафик путем прохождения следующих процедур на сетевом экране (Packet Flow):

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 вовне 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 какой-либо 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

Правило Default SNAT включено на ZyWALL USG по умолчанию.

Функция Virtual Server

Virtual Server делает ресурсы в частной сети за ZyWALL доступными для доступа за пределами сети ZyWALL. Публичный IP-адрес заменяется на локальный IP-адрес. Этот тип NAT не будет выполнять PAT, т.к. все пакеты, полученные на публичный IP-адрес будут просто перенаправлены на локальный IP-адрес.

Публичный IP-адрес заменяется на локальный IP-адрес, при этом, опционально выполняется PAT. Этот тип выполняет более гибкое сопоставление, которое не только подменяет IP-адрес, но и номер порта.

Правило трансляции One to one NAT

Правило One to one NAT (1:1 NAT) - это случай, когда частные серверы сети инициируют сессии для внешних клиентов.

ZyWALL подменяет локальный IP-адрес источника исходящего трафика на публичный IP-адрес, который используется клиентами для доступа к серверу.

Правило трансляции Many 1:1 NAT

Правило Many 1:1 NAT - это случай, когда есть ряд частный серверов сети, которые инициируют сессии для внешних клиентов, и ряд IP-адресов. ZyWALL подменяет локальный IP-адрес источника исходящего трафика от каждого сервера на один из публичных IP-адресов, которые используются внешними клиентами для доступа у серверам.
Many 1:1 NAT работает как несколько правил 1:1 NAT, но упрощает кофигурацию, поскольку нежно создать только одно правило.

Правило трансляции NAT Loopback

Правило 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 у этому серверу.

Правило трансляции Outbound Source NAT

Outbound Source NAT – это механизм, который позволяет заменять IP-адрес источника в пакетах, уходящих IPSec VPN. Используется в случае, если требуется скрыть свои внутренние IP-адреса и в случае, если требуется соединить IPSec VPN туннелем две сети с одинаковой адресацией. Т.к. заменяют адреса источников, необходимо настроить правило Destination NAT, по которому будет определяться соответствие «фальшивого» адреса реальному адресу хоста в локальной сети.
Также применяют Outbound Source NAT в ситуации, когда в локальной сети есть хост, с адресом, не попадающим в указанный на ZyWALL диапазон в local policy и в remote policy на удаленном шлюзе. Если для данного хоста не применять Outbound Source NAT, то удаленная сторона может отбросать пакет от данного хоста, т.к. не будет совпадения и адрес источника пакета.

Правило трансляции Inbound Destination NAT

Inbound Destination NAT – это механизм, который позволяет заменить IP-адрес назначения в пакетах, приходящих по IPSec VPN. Используется в случае, если используется Outbound SNAT. Максимально можно задать до 10 правил Inbound DNAT на 1 VPN туннель.
В случае, если используется Outbound SNAT или Inbound DNAT также необходимо добавить правило в Policy Route и в Firewall.
Процесс SNAT производится после Policy Route, а процесс DNAT производится до Policy Route.

Правило трансляции Inbound Source NAT

Inbound Source NAT – это механизм, который позволяет заменить IP-адрес источника в пакетах, приходящих по IPSec VPN. Используется в

случае, если требуется обезопасить удаленную сеть, т.к. у локального клиента не будет возможности отправить данные в удаленную сеть, т.о. получают односторонний VPN туннель.

Тема 6. Система безопасности межсетевых экранов ZyWALL

Система безопасности межсетевых экранов ZyWALL включает следующие функции *anti-spam, anti-virus, intrusion prevention, web content filtering, bandwidth management, load balancing, vpn, firewall*. Рассмотри их подробнее.

AntiSpam ZyWALL включает в себя:

- Anti-Spam ZyWALL, производства Mailshell, при этом требуется подписка, требуется доступ в Интернет (текст письма никуда не отправляется),
- Поддержка протоколов: POP3 / SMTP,
- Возможные действия: Удалить / Пометить и передать дальше,
- BlackList, WhiteList для ручной настройки.

Технические параметры Anti-Spam

Поддерживаемые протоколы:

- Port 25 (SMTP),
- Port 110 (POP3).

Действия для спама следующие:

- SMTP: (1)Tag and Forward, (2) Discard,
- POP3: (1)Tag and Forward,

Частные правила для Black/White List следующие:

- IP Address (IP адрес и маска),
- Email Address (email адрес),
- MIME Header (заголовок/значение).

Обновления следующие:

- Renew with ZyWALL iCard.

Anti-Spam выполняет следующие действия:

1. Определяет содержание сообщения,
2. Создает подпись и отправляет на rating сервер,
3. Получает ответ на подпись,
4. Принимает решение (Спам или нет).

Общая схема работы Anti-spam

Алгоритм работы функции Anti-Spam следующий:

1) Письмо поступает на ZyWALL

2) ZyWALL проверяет, надо ли применять функцию anti-spam на данном направлении, направление определяется зоной источника и зоной

назначения. 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 попадает ли это письмо под правила White List, если подпадает, то письмо пересылается
4) Если письмо не подпадает под правила White List, то проверятся, подпадает ли оно под правила Black List, если подпадает, значит, данное письмо является спамом и выполняется соответствующее действие
5) Если письмо не подпадает под 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.
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 - списки хостов, хранимые с использованием архитектуры DNS. устройство использует DNSBL серверы для определения того, что является ли данное письмо спамом или нет. Если все DNSBL серверы недоступны в течение определенного тайм-аута (задается администратором), устройство выполните одно их трех действий согласно настройкам.
Anti-Spam - настройка включает в себя:

- Настройка зоновых политик,
- Настройка Black/White List,
- Настройка DNSBL.

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).

Общая схема работы контентной фильтрации

Алгоритм 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 действие какой-либо политики 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,

5) 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. 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.

Content Filtering -настройка включает в себя следующее:

- настройка политик,
- настройка профиля Category Service,
- настройка профиля Custom Service.

Anti-Virus

Anti-Virus – это сканирование в реальном времени, при котором устройство ищет тела вирусов.

Основные настройки Anti-Virus включают следующие действия: включить ☑ функцию Anti-Virus, ☑ протоколы HTTP, FPT, SMTP, POP3, IMAP4.

Создание политики Black/White List включает следующие действия: включить ☑ Black List, включить ☑ White List, заполнить (.avi, .mp3, .exe).

Просмотр сигнатур включает следующие действия:

ONFIGURATION→Anti-X→ Anti-Virus.

IDP (Intrusion Detection & Protection) - система обнаружения и предотвращения вторжений

IDP пресекает вирусный (и не только: P2P клиенты, ICQ, прочие) трафик.

IDP (Intrusion Detection & Protection), 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.

Процесс настройки функции IDP заключается в создании профилей (политик) и последующем назначении профилей любым направлениям передачи трафика. Направление определяется зоной источника и зоной назначения.
Профиль IDP 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».

Custom Signatures - механизм, который позволяет добавлять самодельные сигнатуры в базу. Для добавления сигнатуры необходимо указать несколько параметров, среди которых имя сигнатуры, платформы для которых она актуальна и ряд других, после чего можно приступать к описанию самой сигнатуры, для этого:

1. заполняются значения полей заголовка IP-пакета, которые характерны для данной сигнатуры,
2. заполняются значения полей заголовка TCP/UDP/ICMP-пакета, которые характерны для данной сигнатуры,
3. задается смещение от начала тела пакета и значение строки, которую ZyWALL будет искать в теле TCP/UDP/ICMP-пакета, и нахождение которой является подтверждением наличия данной сигнатуры в теле пакета.

Расположение настройки Custom Signatures следующее:
меню CONFIGURATION→Anti-X→IDP→Custom Signatures

ADP (Anomaly Detection And Prevention)

Функция ADP предназначена для обнаружения аномалий и эффективна против ненормального поведения пакетов, таких как сканирование портов. Обновляется при загрузке новой прошивки.

Endpoint Security (EPS)

Endpoint Security (EPS) проверяет, что система совместима с корпоративной политикой безопасности.

Имеются два критерия проверки Endpoint Security (EPS):

- конечные узлы должны соответствовать, по крайней мере, одному критерию из всех пунктов,
- конечные узлы должны соответствовать всем пунктам проверки.

Endpoint Security Checking позволяет провести проверку компьютеров с различными операционными системами и системами безопасности.

Когда клиент пытается войти в систему, ZyWALL поверяет компьютер клиента с помощью созданных объектов Endpoint Security один за другим. Компьютер клиента должен соответствовать одной из политик Endpoint Security, чтобы получит доступ.

Тема 7. Дополнительные функции межсетевых экранов ZyWALL

Два WAN Порта

При использовании двух внешних портов, имеется возможность организовать доступ к внешним ресурсам через двух независимых провайдеров. При этом можно определить два режима работы ZyWALL:

1. **Active-Passive mode** означает, что только один WAN порт используется одновременно. Когда текущее соединение разрывается, трафик автоматически будет направлен через другое соединение. При установлении соединения по первому разорванному каналу возможен автоматический переход на него обратно (если выбрана соответствующая опция),
2. **Active-Active mode** означает, что оба WAN порта могу использоваться одновременно.

При этом можно определить различные алгоритмы балансировки нагрузки между портами. Все алгоритмы работают на сессиях.

Spillover (Алгоритм переполнения)

Алгоритм переполнения Spillover работает следующим образом: предельное значение нагрузки определяется для основного WAN порта. При достижении этой нагрузки за период (10~600 секунд) начнет использоваться второй WAN порт (для новых сессий). Как только загрузка основного канала упадет ниже предельного, то новые сессии будут открываться на нем.

Пример применения этого алгоритма:

запасной канал более дорогой и используется в качестве дополнительного.

Weighted Round Robin (Циклический взвешенный алгоритм).

Циклический взвешенный алгоритм работает следующим образом: определяется коэффициент загрузки для двух каналов. При этом соотношение определяется для количества сессий пользователей. Например, WAN1:WAN2 = 3:1. Это означает, что количество открытых сессий через WAN1 и WAN2 будут кратны 3:1. При этом реальное распределение нагрузки (коэффициент загрузки канала) не анализируется.

Least Load First

Least Load First (Правило менее загруженной очереди) работает следующим образом: ZyWALL определяет загрузку исходящего потока, входящего и исходящего потока или входящего потока в текущий момент времени.

После чего определяет коэффициент использования канала в соответствии с предельной пропускной способностью канала. Новая сессия открывается через менее загруженный канал.

Например, предельная полоса пропускания на WAN1-512 Kbps, WAN2 - 128 Kbps. Текущая нагрузка каналов WAN1 - 300 Kbps, WAN2 - 100 Kbps. Соответственно коэффициент загрузки канала WAN1 равен 59%, коэффициент загрузки канала WAN2 равен 78 %. Новая сессия будет использовать WAN1.

Отображение статистики

Посредством Web интерфейса в меню Home > Show Statistics можно посмотреть коэффициент использования различных интерфейсов в реальном времени.

Пользователь может выбрать интерфейсы и направление потока данных для графического отображения.

WAN Trunk

WAN Trunk – это механизм, позволяющий объединять несколько внешних каналов в один логический канал. Количество транков может быть от 5 в младших моделях до 15 и более в старших моделях. Для создания WAN Trunk необходимо определить членов данного транка. Членом транка может являться любой интерфейс. Доступно два режима работы каждого интерфейса:

- **Active** – интерфейс, который будет использовать ZyWALL для передачи данных,
- **Passive** – 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. Алгоритмы балансировки нагрузки следующие:

1. **Least Load First** – алгоритм, при котором ZyWALL вычисляет процентную загрузку интерфейса, причем в качестве нагрузки на интерфейс можно учитывать входящий и исходящий трафик, оба потока одновременно. Трафик новой сессии, который необходимо отправить будет отослан в интерфейс с минимальной процентной загрузкой.
2. **Weighted Round Robin - а**лгоритм, основанный на весах интерфейсов. Для каждого интерфейса задается вес (число от 1 до 10) и используя вес ZyWALL будет определять в какой интерфейс отправлять данные новой сессии.
3. **Spillover - а**лгоритм, при котором для каждого интерфейса, включенного в транк, задается пороговое значение скорости. Данные каждой новой сессии будут отправляться в тот интерфейс, на котором пороговое значение скорости не достигнуто и тот интерфейс имеет наименьший порядковый номер в Ланном транке. Например, при наличии интерфейсов WAN 1 и WAN 2 с ограничениями 800 Кб/с и 200 Кб/с соответственно, данные через интерфейс WAN 2 пойдет только в том случае, если интерфейс WAN 1 полностью загружен.

Link Sticking – механизм, позволяющий отправлять данные от донного и того же источника а одному и тому же узлу назначения через один и тот же интерфейс в течение некоторого периода времени. Если включить эту функцию, то второй запрос от отправителя будет отправлен в тот же интерфейс, куда был отправлен первый запрос. Помимо включения функции Link Sticking необходимо указать таймаут, т.е. интервал времени, в течение которого запросы от одного и того же источник к одному и тому же узлу назначения будут отправляться через один и тот же интерфейс.

Резервный туннель

Начиная с микропрограммы версии 4.01 реализована специальная опция, позволяющая задать два адреса удаленного шлюза безопасности: **основной** и **резервный.**

Если основной шлюз окажется недоступным, устройство автоматически переключится на резервный шлюз. Основной и резервный шлюз могут физически представлять собой одно устройство с двумя портами WAN, подключенными к сети Интернет через различные каналы.

Возврат к основному туннелю

Для проверки работоспособности активного туннеля применяются алгоритмы Output Idle Timer, Dead Peer Detection (DPD) и Ping check.

Если туннель до основного шлюза безопасности признается неработоспособным, ZyWALL автоматически устанавливает туннель до резервного шлюза и использует его для передачи данных.

Работая с резервным шлюзом, ZyWALL может производить проверку доступности основного шлюза безопасности, чтобы переключиться на него при появлении такой возможности.
Для проверки доступности основного шлюза один раз в заданный администратором интервал времени ZyWALL отправляет запрос на установку туннеля и, если ответ получен, то считает что канал к основному шлюзу восстановлен.
Сразу после получения ответа, отправляется сообщение об ошибке, которое заставляет основной шлюз прервать процедуру согласования.
Установка туннеля для передачи данных до основного шлюза безопасности будет произведена после истечения времени жизни второй фазы резервного туннеля.
Если ответ от основного шлюза не получен, то ZyWALL повторит попытку еще три раза с указанными задержками, и после четвертой неудачной попытки примет решение оставаться на резервном шлюзе.

Конфигурирование

Конфигурирование резервного шлюза безопасности производится для соответствующего туннеля в разделе настроек первой фазы. Необходимо задать адрес резервного шлюза, а так же указать следует ли возвращаться на основной шлюз при появлении такой возможности и как часто проверять, появилась ли такая возможность.

Device High Availability (Device HA)

Device HA (Device High Availability) функция, которая позволяет использовать несколько устройств ZyWALL в качестве шлюза, обеспечивая резервирование. Режимы работы функции следующие: AP Mode (Active-Passive mode), Legacy Mode.

Device HA AP Mode

Функция **Device HA AP Mode** основывается на протоколе VRRP Virtual Routing Redundancy Protocol, который позволяет использовать несколько шлюзов - один в режиме ведущего (Master), а другой в режиме резервного (Backup). Ведущее устройство выдает себя за виртуальный маршрутизатор. устройства обмениваются специальными пакетами VRRP.
Как только ведомое устройство перестает получать пакеты от ведущего, то оно берет на себя функции ведущего.
В каждый момент времени только один физический маршрутизатор работает от имени виртуального, при этом для пользователей никаких изменений в сети не происходит. Устройства ZyWALL USG используют свою интерпретацию протокола несовместимую с обычными маршрутизаторами с поддержкой VRRP.

Device HA Legacy Mode

Использование Device HA в режиме Legacy Mode позволяет обеспечить резервирование + разделение нагрузки, т.е. создается несколько виртуальных маршрутизаторов, и различным пользователям назначаются различные шлюзы по умолчанию. Т.о. все маршрутизаторы с настроенной функцией Device HA будут задействованы, при этом обеспечивается резервирование.

Механизм BWM

Распределение полосы пропускания

Функция BWM (bandwidth management) устройства ZyWALL включает в себя:

1. Классификатор (Classifier), который классифицирует пакеты на основании правил пользователя, например: IP/Protocol/Port # ,
2. Планировщик (Scheduler), который помещает пакеты в очереди и забирает пакеты из очередей для отправки.

Функция BWM работает для **исходящего** трафика.

Классификатор **Classifier определяет** трафик, удовлетворяющий каким-либо правилам, определенным в BWM, трафик помещается в соответствующее место в дереве классов.

Планировщик **Scheduler** - планировщик выбирает один пакет из класса для последующей обработки и отправки в сеть при условии, что текущий класс не достиг предела полосы пропускания. Планировщик решает, как назначать полосу пропускания различным классам.

Для каждого класса используемая полоса складывается из Назначенной Полосы + Заимствованной Полосы + Maximize Bandwidth Usage.

Maximize Bandwidth Usage (максимально возможная полоса) используется для увеличения пропускной способности класса до уровня полосы канала. Используется незанятая полоса пропускания канала и назначается классу, если данному классу собственной полосы и полосы родителей недостаточно.

Полоса канала назначается классам на основании их приоритета. В этом режиме трафик, который не принадлежит никакому классу, имеет самый низкий приоритет и может вообще не иметь никакой полосы, если назначенным классам она вся необходима.

Схемы планировщика

Существует две схемы, которые могут быть назначены на каждом интерфейсе независимо:

1. **Fairness-based Scheduler (Weighted Round Robin),** взвешенная цикличная схема работает следующим образом**.** Если каким-либо классам необходима дополнительная полоса пропускания в какой-

либо момент времени, то неиспользуемая полоса пропускания будет поделена между ними. При заимствовании (Bandwidth Borrowing) неиспользуемая полоса пропускания разделяется поровну.

2. **Priority-based Scheduler (Priority Round Robin),** приоритетная цикличная схема. Если каким-либо классам необходима дополнительная полоса пропускания в какой-либо момент времени, то неиспользуемая полоса будет поделена в соответствии с приоритетами классов. Вначале будет полностью обслужен наиболее приоритетный класс, затем следующий за ним и т.д.

В операционной системе ZyNOS, наивысший приоритет классов - 7, наименьший приоритет классов - 1.

Настройка через WEB-интерфейс

Перед использованием BWM, необходимо включить ☑ функцию BWM на соответствующем интерфейсе, определить скорость корневого класса этого интерфейса.

Затем необходимо выбрать схему работы планировщика из Priority-Based (PBS) или Fairness-Based (FBS).

В этом же диалоговом окне имеется возможность включить опцию Maximize Bandwidth Usage на интерфейсе.

На закладке Class Setup отображается Дерева классов.

На закладке Monitor отображается экран статистики Bandwidth Management и реальная скорость работы каждого класса в текущий момент времени.

Включение/отключение ☑ Управления полосой пропускания возможно при помощи политик маршрутизации Policy Route (Configuration - Routing - Policy Route). Здесь задается пороговое значение полосы пропускания, которую может использовать политика маршрутизации от 1Kbps до 1Gbps, приоритет трафика попадающего под действие данной политики от 1 (наивысший) до 7, функция **Maximize Bandwidth Usage** позволяющая ZyWALL разделять всю нераспределенную/неиспользуемую полосу пропускания между политиками маршрутизации в случае необходимости.

функция BWM, Policy Routing, Application Patrol

Функция BWM может сочетаться с функцией Policy Routing.

Функция **Application Patrol** позволяет управлять использованием полосы пропускания устройства и управлять возможностью передачи определенного типа трафика до 7-го уровня модели OSI (TCP/UDP порты).

Но приоритет функции Application Patrol ниже, чем у функции Firewall Policy Route.

Контрольные вопросы

1. Что такое Межсетевой экран?
2. Что такое Фильтрация пакетов (packet filtering)?
3. Что такое Proxy-шлюз (applicatio-level gateway)?
4. Что такое Атаки типа DoS?
5. Что такое аутентификация?
6. Что такое целостность данных?
7. Что такое шифрование?
8. Что такое IPSec?
9. Что такое Хеш-функция?
10. Что такое MD5?
11. Что такое SHA1?
12. Что такое симметричный тип шифрования?
13. Что такое асимметричный тип шифрования?
14. Что такое Алгоритм Диффи-Хеллмана DH?
15. Группы Диффи-Хеллмана?
16. Что такое отрытый ключ?
17. Что такое ЭЦП?
18. Что такое IPSec?
19. Что такое ESP?
20. Что такое AH?
21. Что такое SA?
22. Что такое стадия 1 IKE ?
23. Что такое стадия 2 IKE?
24. Что такое Транспортный режим
25. Что такое Туннельный режим
26. Что такое NAT Traversal
27. В чем состоит режим VPN Site-to-Site?
28. Что такое Зомби-туннель?
29. Что такое DPD?
30. Что такое NAT
31. Что такое PAT
32. Что такое SNAT
33. Что такое DNAT
34. Общая схема работы Anti-spam ZyWALL.
35. Что такое Black List?
36. Что такое White List?
37. Алгоритм работы контентной фильтрации.
38. Что такое Anti-Virus?
39. Что такое IDP?
40. Что такое ADP?
41. Что такое Алгоритм Spillover?
42. Что такое алгоритм Weighted Round Robin ?

43. Что такое Least Load First?
44. Что такое Резервный туннель?
45. Что такое Dead Peer Detection?
46. Что такое WAN Trunk?
47. Что такое Device HA?
48. Что такое Device HA AP Mode?
49. Что такое Device HA Legacy Mode?
50. Что такое BWM?

Глоссарий

1. Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.
2. 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.
3. 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)
4. ASAS (Authenex Strong Authentication Server) — RADIUS-сервер, используется для двухфакторной аутентификации.
5. DES (Data Encryption Standart) — симметричный алгоритм шифрования, в котором один ключ используется, как и для шифрования, так и для дешифровки данных. DES разработан фирмой IBM. Для шифрования использует ключ с длиной 56 бит.
6. 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 на много выше.

7. Device HA (Device High Availability) — функция, которая позволяет использовать несколько устройств серии ZyWALL USG в качестве шлюза, тем самым обеспечивание резервирование.
8. 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).
9. DPD (Dead Peer Detecrion) — механизм, с помощью которого IPSec VPN шлюз может проверить работоспособность удаленного шлюза безопасности. (RFC 3706).
10. DSA (Digital Signature Algorithm) — асимметричный алгоритм с использованием открытого ключа и секретного ключа, применяется для создания электронной подписи, но не для шифрования
11. 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)
12. HMAC (Hash Message Authentication Code) — математическая функция, алгоритм которой чаще всего базируется на алгоритме MD5 или SHA-1, однако при расчете хеш-кода используется дополнительный параметр — секретный ключ. (RFC 2104, RFC 2403, RFC 4304)
13. ICV (Integrity check value) — контрольная сумма, некоторое значение, рассчитанное путём применения определённых операций над входными данными. То же самое, что и хеш-код.
14. 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)
15. 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)
16. 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)
17. MAC (Message Authentication Code) — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных.

18. 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 «хеш-кодов» или «дайджестов» сообщений произвольной длины. (RFC 1321)
19. NAS (Network Access Server) — устройство доступа к сети, в контексте решения двухфакторной аутентификации ZyXEL — это шлюз ZyWALL.
20. NAT (Network Address Translation) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса проходящих пакетов. (RFC 1631, RFC 3022)
21. 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)
22. 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)
23. OTP (One Time Password) — пароль, который может быть использован только один раз.
24. PFS (Perfect Forward Secrecy) — функция, позволяющая на второй стадии IKE произвести дополнительный обмен по алгоритму Диффи-Хеллмана, 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.
25. 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)
26. 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)
27. 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 алгоритм шифрования, алгоритм аутентификации и т.д.

28. SHA-1 (Secure Hash Algorithm 1) — алгоритм криптографического хеширования. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом или хеш-кодом сообщения. (RFC 3174)
29. 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 администратором и внутренними ресурсами локальной сети.
30. VPN (Virtual Private Network) — логическая сеть, создаваемая поверх другой сети, например, Интернет, однако обеспечивающая безопасность передачи данных.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра аппаратно-программных комплексов вычислительной техники входит в состав Академии ЛИМТУ Университета ИТМО и имеет более чем 40-летний опыт научно-педагогической деятельности в области профессиональной переподготовки и повышения квалификации специалистов. За последние 20 лет на кафедре прошли обучение более 11 тысяч человек не только из Санкт-Петербурга, но и из различных городов России, а также стран ближнего и дальнего зарубежья. Наши выпускники работают руководителями проектов и начальниками IT-отделов, системными инженерами и системными администраторами, программистами и специалистами по эксплуатации аппаратно-программных комплексов вычислительной техники.

На сегодняшний день на кафедре реализуются следующие направления деятельности:

- подготовка магистров по направлению 09.04.01 «Информатика и вычислительная техника»;
- подготовка бакалавров (без отрыва от производства – вечерняя форма обучения) по направлению 09.03.01 Информатика и вычислительная техника;
- переподготовка специалистов, имеющих высшее образование, с выдачей государственного диплома о дополнительном (к высшему) образовании с присвоением квалификации;
- переподготовка специалистов, имеющих высшее и среднее профессиональное образование с выдачей государственного диплома о переподготовке с правом работы по новой специальности;
- повышение квалификации с выдачей государственного свидетельства (удостоверения)/сертификата Университета ИТМО.

С сентября 2003 года при кафедре функционирует Учебный центр, в котором проводится обучение по программным продуктам фирмы 1С последних версий.

С 2007 года на базе кафедры создан авторизованный Учебный центр фирмы ZyXEL, в котором проводится обучение по теории и практике применения современного сетевого оборудования для построения LAN-WAN сетей с использованием оборудования и технологий ZyXEL.

В 2012 году был создан Авторизованный Учебный центр фирмы QNAP для подготовки сертифицированных специалистов по системам IP-видеонаблюдения и сетевых хранилищ данных.

Программы обучения ориентированы на приобретение устойчивых профессиональных навыков и имеют практическую направленность. Основное время слушатели проводят за компьютером, выполняя большой объем практических заданий. Обучающиеся также получают минимальный объем теоретических знаний, необходимых для грамотного выполнения практических заданий.

Занятия проводятся в пяти специализированных классах, оснащенных современными компьютерами, объединенными в локальную вычислительную сеть с выходом в Интернет. Последние версии программных продуктов ведущих фирм производителей используются не только в учебном процессе, но и выдаются слушателям для установки на домашние компьютеры.

Постоянным заказчиком кафедры на переподготовку специалистов является Департамент федеральной государственной службы занятости населения по Санкт-Петербургу. Обучение слушателей осуществляется также на бюджетной и коммерческой основе.

Светлана Михайловна Платунова

Применение межсетевых экранов фирмы ZyXEL в корпоративных сетях

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе

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