УДК 004.(491+738.5.057.4):65.012.8

НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА НА ШЛЮЗАХ СЕРИИ ZYWALL USG

Нортенко Дмитрий Вячеславович, Масальская Елена Александровна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, dimanortenko@gmail.com

В сети современного предприятия защита от угроз и контроль трафика является одной из основных задач. Устройства защиты сетей масштабов от малого до корпоративного офиса предназначаются для работы в качестве основного либо сегментного шлюза. В данной статье поэтапно расписана настройка межсетевого экрана такого шлюза на примере оборудования серии ZyWALL USG.

Ключевые слова – ZyWALL; шлюз; межсетевой экран; сетевой трафик; фильтрация пакетов.

ВВЕДЕНИЕ

В аппаратном шлюзе серии ZyWALL USG за фильтрацию и контроль проходящего через него трафика отвечает межсетевой экран (Firewall), который, в частности, применяется для разрешения или запрещения работы сервисов (служб), использующих статические номера портов.

ЗОНЫ

При определении направления трафика в правилах межсетевого экрана используются зоны (Zone), представляющие собой объекты, в которых указаны определенные интерфейсы. В зоне может быть указан как один, так и несколько интерфейсов одновременно.

Следовательно, перед началом настройки правил межсетевого экрана необходимо обязательно определить зоны, которые в дальнейшем будут использоваться при настройке правил в устройствах ZyWALL USG. Определенный интерфейс может быть использован только в одной зоне.

Перед настройкой межсетевого экрана для начала нужно убедиться в том, что интерфейсы, которые используются, принадлежат к предустановленным или созданным зонам. Настраиваются зоны в меню Configuration > Network > Zone веб-конфигуратора устройства. Зоны используются в качестве определения направлений при настройке правил Firewall и сервисов Anti-X.

В устройствах есть предустановленные зоны с интерфейсами, которые можна использовать. Если есть необходимость создать свою новую зону и включить в неё определенные интерфейсы, нужно сначала исключить этот интерфейс из предустановленной зоны.

В меню Configuration > Network > Zone выбераем интересующую нас зону из списка System Default и нажимем Edit, чтобы её отредактировать.

В окне Edit Zone в разделе Member List в списке Member находим интерфейс, который необходимо исключить из предустановленной зоны, и переносим его в список Available. Далее создаем нашу новую зону. В меню Configuration > Network > Zone в разделе User Configuration нажимаем Add. В окне Add Zone выбираем из списка Available нужный интерфейс и добавляем его в список Member.

В том случае, если в зоне более одного интерфейса, нужен параметр Block Intra-zone Traffic. Поставив галочку в поле Block Intra-zone Traffic, трафик между интерфейсами, находящимися в одной зоне, начнёт блокироваться.

Если же мы создали новую зону, она не будет автоматически представлена в предустановленных правилах Firewall и прохождение трафика из этой зоны или в эту зону будет зависеть от настроенных правил по умолчанию, где в поле From или To будет одно из значений any или any (Excluding ZyWALL), или по последнему правилу Default.

ПРАВИЛА МЕЖСЕТЕВОГО ЭКРАНА

Настройка правил Firewall осуществляется в меню Configuration > Network > Firewall. Правила Firewall настраиваются по направлениям, то есть по зонам, в которые входят определенные интерфейсы.

Предустановленные правила включают в себя правило по умолчанию Default, находящееся внизу списка правил в разделе Firewall Rule Summary. Это правило нельзя удалить или деактивировать. Для правила по умолчанию Default есть возможность установки значение в поле Access, то есть необходимое действие (allow/deny/reject), которое нужно применить к сетевым пакетам, на которые распространяется данное правила. Исходя из того, что правила Firewall обрабатываются устройством по очереди, под это правило попадут пакеты, не попавшие ни под одно из других правил, находящихся по списку выше.

В меню Configuration > Network > Firewall в разделе General Settings параметр Enable Firewall служит для включения/выключения Firewall.Чтобы включить ставим галочку в поле Enable Firewall.

Allow Asymmetrical Route служит для разрешения/запрещения треугольных асимметричных маршрутов. Чтобы включи ставим галочку в поле Allow Asymmetrical Route. Для создания нового правила межсетевого экрана в меню Configuration > Network > Firewall жмём Add.

ЗНАЧЕНИЕ ПОЛЕЙ В ОКНЕ ADD FIREWALL

Рассмотрим назначение полей в окне Add Firewall Rule, которые необходимо настроить при создании нового правила Firewall. Устанавливаем галочку в поле Enable, чтобы активировать правила.

- From – поле, в котором указываем исходящее направление, по которому создается правило;

- To – поле, указывающее входящее направление, по которому создается правило.
- Description – поле, в котором можно указать описание правила;
- Schedule – поле, в котором можно указать Schedule-объект, созданный ранее в меню Configuration > Object > Schedule. Данный объект определяет расписание работы. В этом случае правило Firewall будет работать в соответствии с ним;
- User – поле, в котором можно выбрать имя пользователя или группу пользователей. Правило будет применяться только к авторизованным пользователям или группам пользователей, если пользователь или группа указаны в этом поле.
- Source – поле, в котором можно указать адрес источника пакетов, к которому должно применяться правило;
- Destination – поле, в котором можно указать адрес назначения пакетов, к которому должно применяться правило;
- Service – поле, в котором можно указать предустановленный или созданный сервис (порт или протокол), к которому должно применяться правило;
- Access – поле, в котором указываем действие, которое будет применяться к сетевому пакету, если он попал под условия правила (allow - разрешить прохождение пакета, deny – отбросить пакет, reject – отбросить пакет с уведомлением на адрес источника);
- Log – поле, в котором можно указать, нужно ли в системные логи делать записи по работе этого правила.

Порядковый номер правил Firewall определяет приоритетность их выполнения. При необходимости изменить приоритетность, то есть порядковый номер, правила, используем элемент Move для изменения порядкового номера.

Чтобы изменить нумерацию правила, выбераем нужное правило и нажимаем на элемент Move после чего указываем новый номер, который мы хотим установить для данного правила, и затем нажимаем клавишу Enter.

С помощью раздела Firewall Rule Summary можно выбирать направления From Zone и To Zone для просмотра правил, подходящих только по указанному направлению.

При создании правила и в списке To Zone существует направление ZyWALL – это направление к самому устройству ZyWALL USG, то есть это трафик, который направляется (адрес назначения) на интерфейс аппаратного шлюза ZyWALL USG.

Также существует направление any (Excluding ZyWALL), которе определяет направление трафика на любую зону, кроме трафика на само устройство. В поле From отсутствует направление для блокировки трафика ZyWALL. Следовательно трафик от ZyWALL USG заблокировать правилами Firewall невозможно.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ZyXEL Security Specialist Ver. 6.0.3 (Електрон. ресурс) / Спосіб доступу: URL: http://www.zyxel.ru/