

Настройки межсетевого экрана

Глобальные настройки

- Отвечать на echo-запросы ICMPv4
- Отвечать на широковещательные запросы ICMPv4
- Обработка IPv4 пакетов, содержащих информацию об исходном маршруте
- Обработка IPv6 пакетов, содержащих информацию об исходном маршруте
- Обработка входящих перенаправляющих сообщений ICMPv4
- Обработка входящих перенаправляющих сообщений ICMPv6
- Использование перенаправляющих сообщений ICMPv4
- Логирование марсианских IPv4 пакетов

Проверка источников по обратному пути

- Строгая
- Мягкая
- Отключена

IPv4 TCP SYN Cookies

Защита от угрозы прерывания по времени в TCP

Обработка пакетов, порожденных другими соединениями (related connections)

- Разрешить (accept)
- Отбросить (drop)
- Отклонить (reject)

Логирование действий над пакетами, порожденными другими соединениями

Обработка пакетов недействительных соединений (invalid connections)

- Разрешить (accept)
- Отбросить (drop)
- Отклонить (reject)

Логирование действий над пакетами недействительных соединений

Псевдонимы

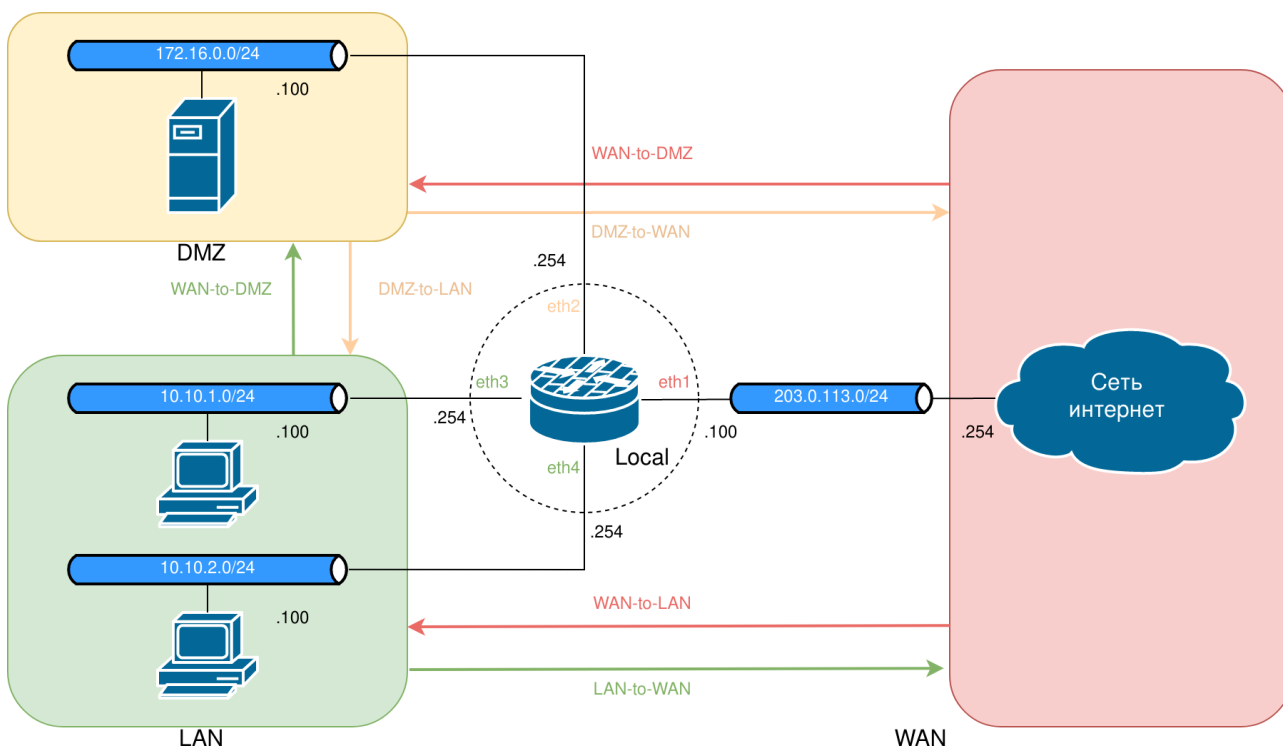
Правила межсетевого экрана

Зоны сети

МЭ

Типичное разделение инфраструктуры компании на три зоны безопасности:

- зона WAN — в данную зону добавляется uplink. Разрешена инициализация соединений с определенными сервисами в зоне DMZ и запрещена инициализация всех соединений с зоной LAN;
- зона LAN — в данную зону добавляются интерфейсы внутренней сети компании. Разрешена установка соединений с зоной WAN и зоной DMZ.
- зона DMZ — в данную зону выносятся сервисы, к которым необходимо осуществлять доступ из зоны WAN. Запрещены исходящие соединения в зону LAN.
- **Зона EDGE** — зона для подключения доверенных сетей для администрирования



пример реализации данной концепции:

- Имеются три транзитных зоны (то есть точки, где трафик проходит через маршрутизатор): закрытая зона, демилитаризованная зона (DMZ) и общедоступная зона.
- Интерфейс eth1 лежит в общедоступной зоне; eth2 лежит в DMZ; eth3 и eth4 лежат в закрытой зоне.
- Стрелки из одной зоны в другую представляют политики фильтрации трафика, применяемые к трафику, передаваемому между зонами.
- Трафик, передаваемый между 10.10.3.0/24 и 10.10.4.0/24, остаётся в одной и той же зоне безопасности, так что трафик между этими подсетями передается без фильтрации.

Помимо трех транзитных зон, на рисунке ниже есть и **четвёртая зона** – **локальная зона, описывающая сам межсетевой экран**

Начальная настройка IP-адресации#

На рисунке выше приведена схема сетевой адресации внутри организации. Для удобства данная схема представлена в виде таблицы ниже.

Подсеть	IP адрес	Устройство	Зона
10.10.101.0/24	dhcp	ARMA Стена#eth0	EDGE
10.10.5.0/24	10.10.5.254	ARMA Стена#eth1	WAN
	10.10.5.1	Шлюз провайдера	WAN
172.16.1.0/24	172.16.1.100	Сервер организации	DMZ
	172.16.1.1	ARMA Стена#eth2	DMZ
10.10.1.0/24	192.168.1.100	APM1	LAN
	192.168.1.1	ARMA Стена#eth3	LAN
10.10.2.0/24	192.168.2.100	APM2	LAN
	10.10.2.254	ARMA Стена#eth4	LAN

Для настройки данных подсетей в ARMA Стена перейдите в конфигурационный режим и

Настройки интерфейсов							
+ Добавить □ Удалить							
Введите текст							
Наименование	Физический инте...	Тип	Статус	IP адрес	MAC адрес	Состояние	Описание
eth0	-	Ethernet: Физический	Активен	10.10.101.7/24	08:00:27:69:6f:0c	Подключено	EDGE (admin function)
eth1	-	Ethernet: Физический	Активен	172.16.1.1/24	08:00:27:63:68:cc	Подключено	DMZ
eth2	-	Ethernet: Физический	Активен	192.168.1.1/24	08:00:27:06:c8:7b	Подключено	LAN
eth3	-	Ethernet: Физический	Активен	10.10.5.254/24	08:00:27:76:26:e6	Подключено	WAN

Создание транзитных зон и добавление в них сетевых интерфейсов

```
set firewall zone EDGE local-zone
set firewall zone EDGE description „ EDGE zone“
set firewall zone LAN interface eth2
set firewall zone LAN description „ LAN zone“
set firewall zone DMZ interface eth1
set firewall zone DMZ description „DMZ zone“
set firewall zone WAN interface eth3
set firewall zone WAN description „ WAN zone“

show firewall zone
```

```

ethernet eth0 {
  address dhcp
  description "Uplink (admin function)"
  hw-id 08:00:27:69:6f:0c
  offload {
    gro
    gso
    sg
    tso
  }
}
ethernet eth1 {
  address 172.16.1.1/24
  description DMZ
  hw-id 08:00:27:63:68:cc
  vif 0 {
    address dhcp
  }
}
ethernet eth2 {
  address 192.168.1.1/24
  description LAN
  hw-id 08:00:27:06:c8:7b
  vif 0 {

```

```

  address dhcp
  }
}
ethernet eth3 {
  address 10.10.5.254/24
  description WAN
  hw-id 08:00:27:76:26:e6
  vif 0 {
    address dhcp
  }
}
loopback lo {
}
[edit]

```

Настройка базовых политик фильтрации#

Перед началом настройки сложных правил фильтрации, которые описывают различные условия прохождения трафика будет полезно создать простые правила, явно запрещающие или разрешающие проходящий трафик в определенную зону.

Для этого необходимо настроить следующие политики:

- "ALL_ACCEPT" — безусловно разрешающая политика для передачи трафика между транзитными зонами.
- "ALLOW_RESPONSE" — политика на основе состояния соединения, разрешающая только ответный трафик;
- "ALL_DROP" — безусловная запрещающая политика для передачи трафика между транзитными зонами и локальной зоной

Создание узла конфигурации (набора правил) для политики ALL_ACCEPT и ввод описания для неё

```

set firewall ipv4 name ALL_ACCEPT
set firewall ipv4 name ALL_ACCEPT description "allow all traffic"

```

Создание правила для принятия всего трафика, передаваемого в общедоступную зону:

```

set firewall ipv4 name ALL_ACCEPT default-action accept

```

Пример – Создание политики разрешающий ответный трафик

1) Создание правила фильтрации 10 в наборе правил STATE-GOOD для разрешения прохождения только трафика, исходящего из этой зоны (т.е. ранее установленные сеансы и связанный с ними трафик): разрешения прохождения только трафика, исходящего из этой зоны (т.е. ранее установленные сеансы и связанный с ними трафик):

```
#создаем набор правил STATE-GOOD
set firewall ipv4 name STATE-GOOD
#
#разрешаются
set firewall ipv4 name STATE-GOOD rule 10 action accept
#установленные оединения;
rset firewall ipv4 name STATE-GOOD rule 10 state established
#связанные соединения
set firewall ipv4 name STATE-GOOD rule 10 state related
set firewall ipv4 name STATE-GOOD rule 10 protocol all
```

2) Создание узла конфигурации для политики ALLOW_RESPONSE и ввод описания для неё

```
#создаем набор правил ALLOW_RESPONSE
set firewall ipv4 name ALLOW_RESPONSE
set firewall ipv4 name ALLOW_RESPONSE description "filter traffic to LAN zone"
```

3) Создание правила rule 10 для политики межсетевого экранирования ALLOW_RESPONSE. Это правило разрешает трафик, соответствующий указанным критериям:

```
#rule 10 action accept
set firewall ipv4 name ALLOW_RESPONSE rule 10 action accept
```

4) Применение фильтра STATE-GOOD к политике межсетевого экрана ALLOW_RESPONSE:

```
set firewall ipv4 name ALLOW_RESPONSE rule 10 action jump
set firewall ipv4 name ALLOW_RESPONSE rule 10 jump-target STATE-GOOD
```

ПРИМЕР – СОЗДАНИЕ БЕЗУСЛОВНО ЗАПРЕЩАЮЩЕЙ ПОЛИТИКИ#

1) Создание узла конфигурации для политики ALL_ACCEPT и ввод описания для неё:

```
set firewall ipv4 name ALL_DROP description "drop all traffic"
```

2) Создание правила для принятия всего трафика, передаваемого в общедоступную зону:

```
set firewall ipv4 name ALL_DROP default-action drop  
commit
```

Применение базовых политик фильтрации#

После создания базовых политик фильтрации необходимо определить между какими зонами они будут применяться. Необходимо помнить, что политики применяются для трафика, входящего в определенную зону.

- для такого трафика, который передается из зоны А в зону В следующим образом:

```
set firewall zone B from A firewall name Кастомное_правило
```

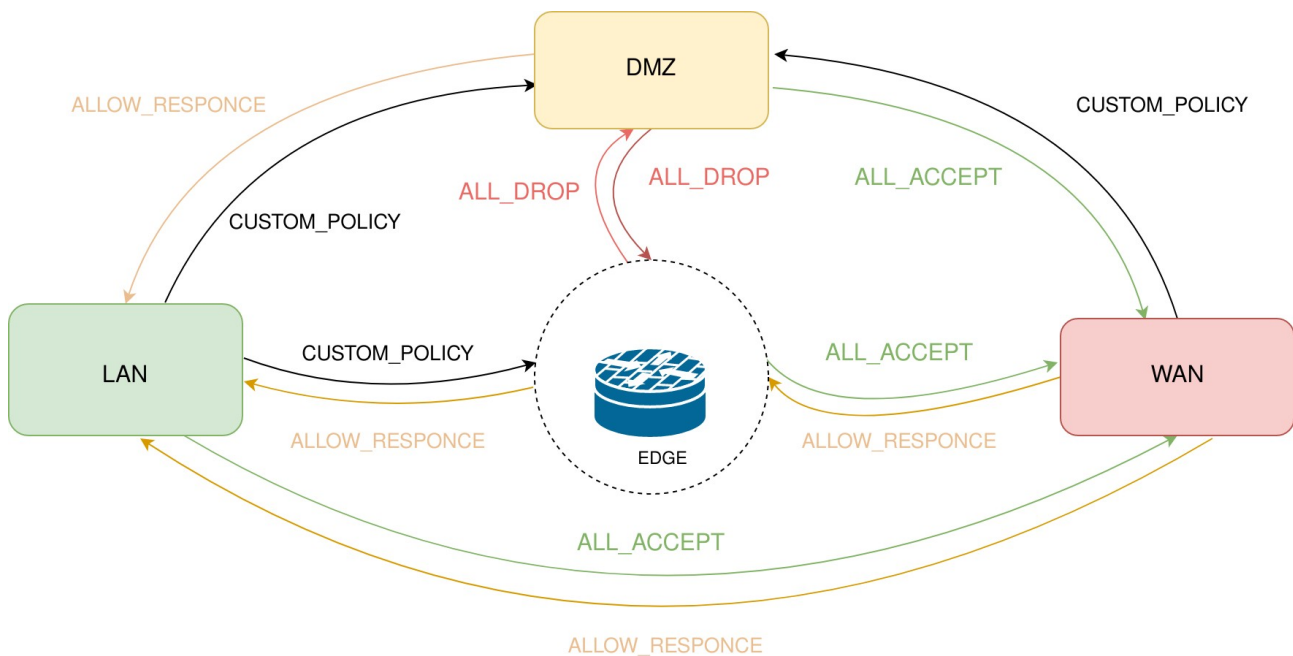
- для такого трафика, который передается из зоны В в зону F следующим образом:

```
set firewall zone A from B firewall name Кастомное_правило
```

Направление трафика, к которому будут применены базовые политики представлено на рисунке ниже.

Согласно данному рисунку получается следующий набор базовых политик фильтрации трафика:

- Разрешен весь трафик LAN-to-WAN, EDGE-to-WAN, DMZ-to-WAN.
- Разрешен только ответный трафик WAN-to-LAN, EDGE-to-LAN, WAN-to-EDGE, DMZ-to-LAN.
- Запрещен весь трафик DMZ-to-EDGE, EDGE-to-DMZ.



Для направления трафика, который помечен как CUSTOM_POLICY будут применены более сложные правила фильтрации.

1) Разрешение передачи любого трафика из зоны LAN в зону WAN:

```
set firewall zone WAN from LAN firewall name ALL_ACCEPT
```

2) Разрешение передачи любого трафика из локальной зоны EDGE в зону WAN

```
set firewall zone WAN from EDGE firewall name ALL_ACCEPT
```

3) Разрешение передачи любого трафика из зоны DMZ в зону WAN:

```
set firewall zone WAN from DMZ firewall name ALL_ACCEPT
```

4) Разрешение только ответного трафика из зоны WAN в зону LAN:

```
set firewall zone LAN from WAN firewall name ALLOW_RESPONSE
```

5) Разрешение только ответного трафика из локальной зоны EDGE в зону LAN

```
set firewall zone LAN from EDGE firewall name ALLOW_RESPONSE
```

6) Разрешение только ответного трафика из зоны WAN в локальную зону EDGE

```
set firewall zone EDGE from WAN firewall name ALLOW_RESPONSE
```

7) Разрешение только ответного трафика из зоны DMZ в зону LAN

```
set firewall zone LAN from DMZ firewall name ALLOW_RESPONSE
```

8) Запрет любого трафика из локальной зоны EDGE в зону DMZ

```
set firewall zone DMZ from EDGE firewall name ALL_DROP
```

9) Запрет любого трафика из зоны DMZ в локальную зону EDGE:

```
set firewall zone EDGE from DMZ name firewall ALL_DROP
```

10) Применение конфигурации

```
commit
```

Просмотр примененной конфигурации

```
show firewall zone
```

Обратите внимание, что после применения данной конфигурации, передача трафика между транзитными зонами будет запрещена. Это связано с тем, что для каждой транзитной зоны по умолчанию (если пакет не попадает ни под одну из политик) используется действие drop.

Создание и применение специальных политик фильтрации

Теперь создаются более сложные политики фильтрации, описывающие прохождения трафика в следующих направлениях:

- WAN-to-DMZ – политика, разрешающая доступ из интернета с помощью протоколов HTTP, HTTPS на сервер в зоне DMZ. Дополнительно разрешается весь ICMP трафик.
- LAN-to-DMZ – политика, разрешающая доступ из зоны LAN в зону DMZ с помощью протоколов HTTP и HTTPS а так же FTP и SSH . Весь ICMP трафик так же разрешен.
- LAN-to-EDGE – политика, разрешающая доступ с помощью протокола SSH только для определенного адреса отправителя.

Первоначально создадим необходимые фильтры:

- WAN_SERVICE_PORT – перечень портов, доступ к которым разрешен из публичной сети (в данном случае из зоны WAN).
- LAN_SERVICE_PORT – порты, доступ к которым разрешен из частной сети (зоны LAN).
- ICMP – фильтр, описывающий ICMP трафик.

ПРИМЕР – СОЗДАНИЕ ФИЛЬТРА WAN_SERVICE_PORT

1) Вначале создаем порт-группу, в которую добавляются все необходимые порты. Данный метод удобнее простого описания списка портов в правиле фильтрации, поскольку позволяет гибко управлять содержимым группы без необходимости редактирования фильтра:

```
set firewall group <typealias> <name>
```

```
set firewall group port-group PUBLIC_SERVICE_PORT
```

```
set firewall group port-group PUBLIC_SERVICE_PORT port http
```

```
set firewall group port-group PUBLIC_SERVICE_PORT port https
```

Добавление псевдонима Отменить Сохранить

Наименование*

Тип*

Протокол Порт Диапазон портов

Протокол*

Протокол Порт Диапазон портов

Протокол*

2) Теперь создается фильтр WAN_SERVICE_PORT, для которого в качестве портов назначения трафика выбирается ранее созданная группа:

Для добавления псевдонима в правило МЭ необходимо ввести команду, в зависимости от направления трафика:

```
set firewall <type> <category> rule <num> source group <typealias> [<name> | <!name>]
```

- «source» – источник
- «destination» – назначение.
- <name> – имя псевдонима;
- <!name> – имя псевдонима с отрицанием.

#Доступ разрешить к портам группы PUBLIC_SERVICE_PORT

```
set firewall ipv4 name WAN_SERVICE_PORT rule 10 action accept
```

```
set firewall ipv4 name WAN_SERVICE_PORT rule 10 destination group port group PUBLIC_SERVICE_PORT
```

3) Синтаксис системы конфигурации требует не только указание числового или символьного обозначения портов, но и протокол, относящийся к данным портам. В данном случае порты HTTP и HTTPS работают поверх протокола TCP:

```
set firewall ipv4 name WAN_SERVICE_PORT rule 10 protocol tcp
```

```
set firewall ipv4 name WAN_SERVICE_PORT description 'Ports to which connections can be established from an WAN zone'
```

```
commit
```

The screenshot shows the configuration interface for a firewall rule named "Правило 10". At the top, there are buttons for "Отменить" (Cancel), "Сохранить" (Save), and a refresh icon. The rule is currently enabled, as indicated by the "Статус правила" (Rule Status) toggle switch. The configuration fields are as follows:

- Набор*** (Set): ALLOW_RESPONSE (IPv4)
- Тип*** (Type): ipv4. A note below indicates "Тип наследуется от набора" (Type is inherited from the set).
- Приоритет*** (Priority): 10
- Логирование** (Logging): Disabled (toggle switch).
- Действие*** (Action): Перейти (jump)
- Переадресация*** (Redirection): STATE-GOOD

Аналогичным образом создается правило фильтрации для доступа к сервисным портам из зоны LAN.

ПРИМЕР – СОЗДАНИЕ ФИЛЬТРА LAN_SERVICE_PORT

1) Аналогично с предыдущим примером создается порт-группа PRIVATE_SERVICE_PORT в которую помимо портов HTTP и HTTPS добавляются еще порты FTP и SSH:

```
set firewall group port-group PRIVATE_SERVICE_PORT
set firewall group port-group PRIVATE_SERVICE_PORT port http
set firewall group port-group PRIVATE_SERVICE_PORT port https
set firewall group port-group PRIVATE_SERVICE_PORT port ftp
set firewall group port-group PRIVATE_SERVICE_PORT port ssh
```

Псевдонимы		
Наименование	Тип	Состав группы
<input type="radio"/> PRIVATE_SERVICE_PORT	Порты	http, https, ftp, ssh
<input type="radio"/> PUBLIC_SERVICE_PORT	Порты	http, https

2) Также, аналогично предыдущему примеру создается правило фильтрации LAN_SERVICE_PORT, в которое добавляется данная группа,

```
set firewall ipv4 name LAN_SERVICE_PORT rule 10 action accept
set firewall ipv4 name LAN_SERVICE_PORT rule 10 destination group port group PRIVATE_SERVICE_PORT
```

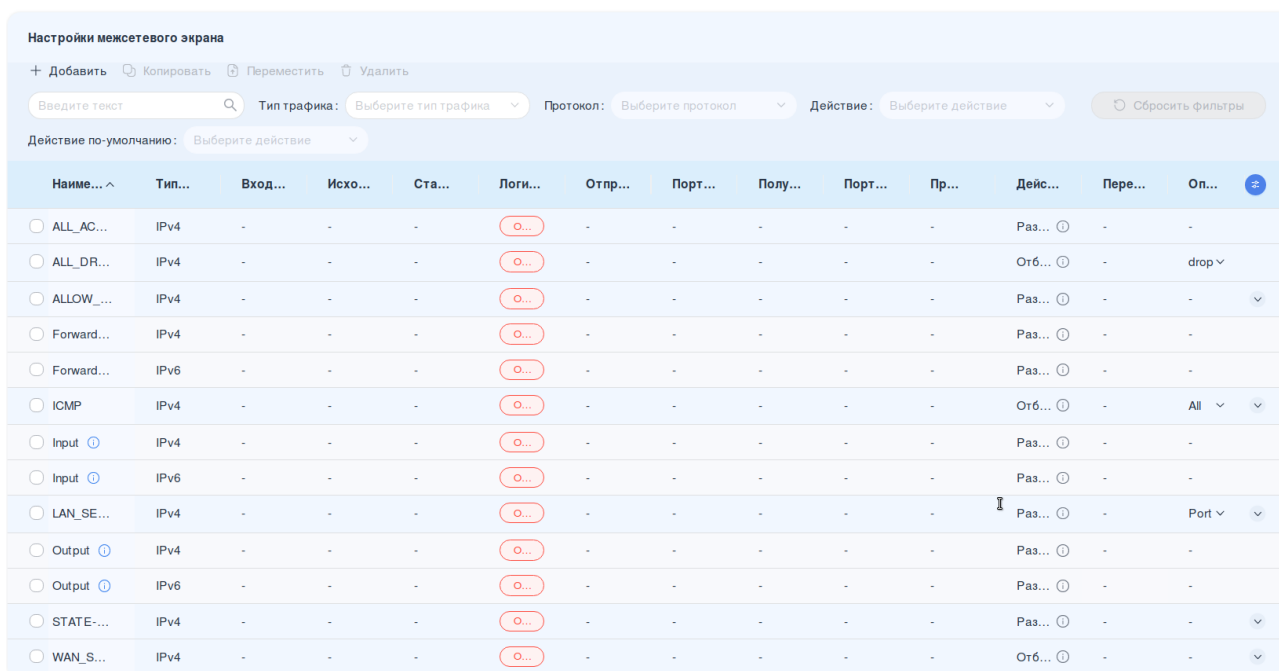
3) Все порты работают поверх протокола TCP

```
set firewall ipv4 name LAN_SERVICE_PORT rule 10 protocol tcp
set firewall ipv4 name LAN_SERVICE_PORT description „Ports to which connections can be established from an LAN zone“
commit
```

И последним этапом в настройке фильтров будет описание ICMP трафика.

ПРИМЕР – ФИЛЬТР ДЛЯ ICMP ТРАФИКА

Для ICMP трафика выбирается любой тип сообщений. Детальная настройка разрешений для ICMP трафика выходит за рамки данного документа:



The screenshot shows the Mikrotik WinBox interface for configuring a firewall filter. The title is "Настройки межсетевого экрана". At the top, there are buttons for "Добавить", "Копировать", "Переместить", and "Удалить". Below these are search and filter options: "Введите текст" (search), "Тип трафика: Выберите тип трафика" (dropdown), "Протокол: Выберите протокол" (dropdown), "Действие: Выберите действие" (dropdown), and "Сбросить фильтры" (button). A "Действие по умолчанию" dropdown is also present. The main part of the image is a table listing various firewall rules. The "ICMP" rule is highlighted in blue. The table columns are: Наиме..., Тип..., Вход..., Исхо..., Ста..., Логи..., Отпр..., Порт..., Полу..., Порт..., Пр..., Дейс..., Пере..., Оп... (with a search icon). The "ICMP" row shows: ALL_AC..., IPv4, -, -, -, (red circle with "0..."), -, -, -, -, -, Раз..., -, -.

Наиме...	Тип...	Вход...	Исхо...	Ста...	Логи...	Отпр...	Порт...	Полу...	Порт...	Пр...	Дейс...	Пере...	Оп...
<input type="radio"/> ALL_AC...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> ALL_DR...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Отб...	-	drop
<input type="radio"/> ALLOW_...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> Forward...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> Forward...	IPv6	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> ICMP	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Отб...	-	All
<input type="radio"/> Input	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> Input	IPv6	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> LAN_SE...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	Port
<input type="radio"/> Output	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> Output	IPv6	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> STATE-...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Раз...	-	-
<input type="radio"/> WAN_S...	IPv4	-	-	-	(red circle with "0...")	-	-	-	-	-	Отб...	-	-

```
admin@ngfwos# sho firewall ipv4 name ICMP
description "All ICMP traffi"
rule 10 {
    action accept
    disable
    protocol all
}
[edit]
admin@ngfwos# _
```

set firewall ipv4 name ICMP

set firewall ipv4 name ICMP rule 10 icmp type all

set firewall ipv4 name ICMP description "All ICMP traffic"

После того как требуемые фильтры были созданы, осталось применить их к политикам фильтрации трафика между зонами.

Первоначально описывается политика, регулирующая доступ из зоны WAN в зону DMZ.

ПРИМЕР – НАСТРОЙКА ПОЛИТИКИ WAN-TO-DMZ

1) Создание политики межсетевого экранирования WAN-to-DMZ . К трафику, который не попадает под созданные правила, применяется стандартное действие drop (по умолчанию). Для логирования этого трафика, добавляется соответствующая настройка:

```
set firewall ipv4 name WAN-to-DMZ
set firewall ipv4 name WAN-to-DMZ default-action drop
set firewall ipv4 name WAN-to-DMZ default-log
```

К созданной политике межсетевого экранирования добавляется описание:

```
set firewall ipv4 name WAN-to-DMZ description "Allow only destination HTTP,HTTPS and ICMP traffic"
```

2) Добавление правила 10, в котором в качестве портов назначения указаны HTTP и HTTPS:

```
set firewall ipv4 name WAN-to-DMZ rule 10 action jump
set firewall ipv4 name WAN-to-DMZ rule 10 jump-target WAN_SERVICE_PORT
```

Если трафик попадает под данный фильтр, то он разрешается:

```
set firewall ipv4 name WAN-to-DMZ rule 10 action accept
```

4) Создание правила 20, в котором описан ICMP трафик

```
set firewall ipv4 name WAN-to-DMZ rule 20 action jump
set firewall ipv4 name WAN-to-DMZ rule 20 jump-target ICMP
```

Если трафик попадает под данный фильтр — он разрешается:

```
set firewall ipv4 name WAN-to-DMZ rule 20 action accept
```

5) Применение изменений:

```
commit
```

```
admin@ngfwos# show firewall ipv4 name WAN-to-DMZ
default-action drop
default-log
description "Allow only destination HTTP,HTTPS and ICMP traffic"
rule 10 {
    action jump
    jump-target ICMP
}
rule 20 {
    action jump
    jump-target WAN_SERVICE_PORT
}
[edit]
```

6) Применение политики межсетевого экранирования, для трафика передаваемого из firewall зоны WAN в зону DMZ:

```
set firewall zone DMZ from WAN firewall name WAN-to-DMZ
commit
```

Теперь описывается политика межсетевого экранирования для трафика, передаваемого из зоны LAN в зону DMZ.

ПРИМЕР – НАСТРОЙКА ПОЛИТИКИ LAN-to-DMZ

1) Аналогично предыдущему примеру создается политика LAN-to-DMZ, Аналогично прошлому примеру, весь трафик, не попадающий под разрешающие правила – запрещается (? отбросить), а запись о нем заносится в системный журнал:

```
set firewall ipv4 name LAN-to-DMZ default-action drop
set firewall ipv4 name LAN-to-DMZ filter default-log
set firewall ipv4 name LAN-to-DMZ description "Allow only destination
HTTP,HTTPS,FTP,SSH and ICMP traffic"
```

2) в правиле 10 описывается трафик, который предназначен для служб SSH, FTP, HTTP и HTTPS:

```
set firewall ipv4 name LAN-to-DMZ
set firewall ipv4 name LAN-to-DMZ rule 10 action jump
set firewall ipv4 name LAN-to-DMZ rule 10 jump-target LAN_SERVICE_PORT
```

Трафик, попадающий под это правило разрешается:

```
set firewall ipv4 name LAN-to-DMZ rule 10 action accept
```

3) Правило 20 соответствует прошлому примеру:

```
set firewall ipv4 name LAN-to-DMZ rule 20 action jump
set firewall ipv4 name LAN-to-DMZ rule rule 20 jump-target ICMP
```

Трафик, попадающий под это правило разрешается:

```
set firewall ipv4 name LAN-to-DMZ rule 20 action accept
```

4) Применение изменений:

```
commit
```

```
admin@ngfwos# show firewall ipv4 name LAN-to-DMZ
  default-action drop
  default-log
  description "Allow only destination HTTP,HTTPS,FTP,SSH and ICMP traffic"
  rule 10 {
    action jump
    jump-target LAN_SERVICE_PORT
  }
[edit]
```

5) Применение политики межсетевого экранирования, для трафика передаваемого из зоны LAN в зону DMZ:

```
set firewall zone DMZ from LAN firewall name LAN-to-DMZ
```

```
commit
```

Завершающим этапом настройки будет ограничения доступа к ARMA Стена из зоны LAN. Данная настройка несет потенциальный риск потерять управления в случае ошибочных действий. Для примера доступ по SSH разрешен только с устройства 10.10.1.100.

ПРИМЕР – НАСТРОЙКА ПОЛИТИКИ LAN-to-EDGE

1) Создание политики фильтрации, который описывает возможность подключения к ARMA Стена через протокол SSH только с устройства 10.10.1.100. В дальнейшем, можно использовать группу адресов для описания нескольких устройств, с которых возможно управление:

?проверить?

```
set firewall ipv4 name      EDGE-MGMT
set firewall ipv4 name      EDGE-MGMT default-action accept
set firewall ipv4 name      EDGE-MGMT rule 10 port ssh
set firewall ipv4 name      EDGE-MGMT rule 10 protocol tcp
set firewall ipv4 name      EDGE-MGMT rule 10 source address 10.10.101.96
commit
```

2) Создание политики межсетевого экранирования LAN-to-EDGE

```
set firewall ipv4 name      LAN-to-EDGE
```

Весь явно не разрешенный трафик запрещен и запись о нем заносится в системный журнал

```
set firewall ipv4 LAN-to-EDGE default-action drop
set firewall ipv4 LAN-to-EDGE filter default-log
```

3) Создание правила, которое ограничивает доступ к ARMA Стена:

```
set firewall ipv4 name      LAN-to-EDGE rule 10 action jump
set firewall ipv4 name      LAN-to-EDGE rule 10 jump-target  EDGE-MGMT
```

Трафик, попадающий под это правило разрешается:

```
set firewall ipv4 name      LAN-to-EDGE rule 10 action accept
```

4) Создание правила, разрешающего ICMP трафик:

```
set firewall ipv4 LAN-to-EDGE rule 20 match filter ICMP
set firewall ipv4 LAN-to-EDGE rule 20 action accept
set firewall ipv4 name      LAN-to-EDGE rule 20 action accept
```

5) Для данной политики задается описание:

```
set firewall ipv4 LAN-to-EDGE description "Allow SSH connection only from 10.10.1.100"
Commit
```

```
admin@ngfwos# commit
[edit]
admin@ngfwos# show firewall ipv4 name LAN-to-DMZ
default-action drop
default-log
description "Allow only destination HTTP,HTTPS,FTP,SSH and ICMP traffic"
rule 10 {
    action jump
    jump-target EDGE-MGMT
}
[edit]
```

6) Применение политики межсетевого экранирования, для трафика передаваемого из зоны LAN в зону локальную EDGE

```
set firewall zone EDGE from LAN firewall name LAN-to-EDGE
commit
```

Настройка межсетевого экрана на основе зон завершена и теперь необходимо убедиться в его правильности с помощью проверки прохождения трафика.

Проверка#

Конечная проверка будет включать в себя генерацию ICMP трафика в следующих направлениях:

- Из LAN в LAN — передача трафика внутри одной зоны — должен быть разрешен;
- Из LAN в WAN — доступ в интернет для локальных пользователей — должен быть разрешен;
- Из WAN в LAN — проверка возможности установки соединения из интернета в локальную сеть — должен быть запрещен;
- Из WAN в DMZ — проверка доступности внутренних сервисов из интернета — должен быть разрешен;
- Из DMZ в EDGE — доступ из сервисной сети за сам маршрутизатор — должен быть запрещен;
- Из LAN в EDGE — проверка возможности управления устройством из локальной сети — должен быть разрешен;
- Из LAN в DMZ — проверка доступности внутренних сервисов внутри сети — должен быть разрешен.

```
set firewall ipv4 name allow rule 10 action accept
```

разрешающее сетевой трафик для частной подсети 192.168.0.0/16, используемой на данном предприятии.

```
set firewall ipv4 name allow rule 10 destination address '192.168.5.0/24'
```

назначение действия по умолчанию, выполняемого в случае, если сетевой пакет не удовлетворяет критериям ни одного правила

```
set firewall ipv4 name allow default-action accept
```

```
set zone-policy zone LAN from WAN firewall name allow
```

```
set zone-policy zone WAN from LAN firewall name allow
```

где «LAN» и «WAN» – имена зон; «eth0» – интерфейс с доступом к сети Интернет; «allow» – имя набора правил.

.

Отправление ARMA Стена ответов на локальные ICMP-запросы — включено (по ум)

```
set firewall global-options all-ping enable
```

Отправление ARMA Стена ответов на широковещательные ICMP-запросы (выкл по ум)

```
set firewall global-options broadcast-ping disable
```

```
#Разрешить на внутреннем интерфейсе весь трафик из локальной сети (входящий)
```

```
set firewall ipv4 input filter
```

```
# Устанавливаем политики по умолчанию:
```

```
# ?Входящий трафик — сбрасывать «drop»; Исходящий — разрешать
```

```
set firewall ipv4 input filter default-action 'drop'
```

```
set firewall ipv4 output filter default-action 'accept'
```

```
НАБОР ПРАВИЛ
```

```
set firewall ipv4 <type> name имя_набора
```

```
# Правило – по умолчанию для входящих соединений - Разрешить транзитные соединения
```

```
set firewall ipv4 forward filter default-action 'accept'
```

```
set firewall ipv4 forward filter default-log
```

```
# Правило 10 - Разрешить перенаправление трафика с внутренней сети наружу, для частной подсети 192.168.5.0/24, используемой на данном предприятии.
```

```
set firewall ipv4 forward filter rule 10 action 'accept'
```

```
set firewall ipv4 forward filter rule 10 destination address '192.168.5.0/24'
```

```
# Правило 20 - блокирует весь сетевой трафик, за исключением пакетов, содержащих IP-адреса, находящиеся в Российской Федерации.
```

```
set firewall ipv4 forward filter rule 20 action 'drop'
```

```
set firewall ipv4 forward filter rule 20 destination geoip country-code 'ru'
```

```
set firewall ipv4 forward filter rule 20 destination geoip inverse-match
```

```
set firewall ipv4 forward filter rule 20 log
```

```
#Правило 30 - # Позволяем два, наиболее безопасных типа пинга 0 и 8 (входящие)
```

```
set firewall ipv4 <category> rule 30 type-name echo-reply
```

```
set firewall ipv4 <category> rule 30 type-name echo-request
```

```
# Правило 30 -40 - Разрешить перенаправление только тех пакетов с внешней сети внутрь, которые уже являются частью имеющихся соединений и связанных
```

```
set firewall ipv4 forward filter rule 40 state established
```

```
set firewall ipv4 forward filter rule 50 state related
```

```
# Выполняем трансляцию сетевых адресов, принадлежащих локальной сети NAT
```


Кэширующий прокси сервер

1) Для настройки переадресации DNS введены следующие команды:

```
set system name-server 8.8.8.8
set service dns forwarding cache-size 500
set service dns forwarding listen-address 192.168.5.1
set service dns forwarding allow-from 192.168.5.0/24
set service dns forwarding name-server 8.8.8.8
```

2) Настройка правил NAT, преобразующего адрес источника:

```
set nat source rule 1 outbound-interface eth1
set nat source rule 1 source address 192.168.5.0/24
set nat source rule 1 translation address masquerade
```

где «outbound-interface» – для интерфейсов, используемых для внешнего трафика:
для правил SNAT адрес источника пакетов будет заменён адресом, указанным в
команде «translation»

«inbound-interface» – для интерфейсов, используемых для внутреннего трафика

Для просмотра конфигурации NAT необходимо ввести команду «show nat».

где «eth1» – интерфейс с доступом к сети интернет;

«192.168.5.0/24» – адрес сети интерфейса «eth1», который будет подменяться IP-адресом
интерфейса «eth0».

3)

Для настройки МЭ введена следующая команда:

```
set firewall all-ping enable
```

Для создания DHCP-сервера на ARMA Стена необходимо указать подсети и задать диапазон выдаваемых IP-адресов с помощью ввода следующих команд:

```
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24
set service dhcp-server shared-network-name Net1 subnet 192.168.5.0/24 range 0 start 192.168.5.10
set service dhcp-server shared-network-name Net1 subnet 192.168.5.0/24 range 0 stop 192.168.5.100
```

Указание интерфейса для прослушивания запросов от клиентов DHCP ()

4) Настройка прокси

Для настройки прокси-сервера необходимо ввести следующие команды:

```
set service webproxy listen-address 192.168.5.1
set service webproxy listen-address 192.168.5.1
port 3128 set service webproxy listen-address 192.168.4.1
disable-transparent
```

(с.38

Настройка устройств кластера

МЭ

Требуется разрешить для служб

nginx, pgadmin, postgres, zabbix-web, zabbix, django

1) Для работы веб-сервера Nginx необходимо разрешить использование следующих портов и протоколов:

- Порт 22 (SSH). Протокол удалённого доступа к серверу, обеспечивает зашифрованное соединение и аутентификацию пользователя. Открыв этот порт, можно подключаться к серверу с помощью SSH, что необходимо для администрирования и управления.
- Порт 80 (HTTP). Обеспечивает обычное соединение HTTP.
- Порт 443 (HTTPS). Защищённое соединение HTTPS с использованием SSL/TLS-шифрования.

При настройке брандмауэра для Nginx важно закрыть все порты, кроме необходимых, чтобы обеспечить безопасность веб-сервера.

Некоторые параметры могут отличаться в зависимости от дистрибутива.

2) По умолчанию для работы pgAdmin используется порт 5432.

Для связи между клиентами и серверами PostgreSQL, на котором работает pgAdmin, поддерживаются протоколы TCP/IP и сокеты домена Unix.

Если брандмауэр настроен так, что блокирует HTTP-подключения, это может препятствовать работе pgAdmin. В таком случае можно попробовать изменить номер порта, назначенный операционной системой, в настройках pgAdmin. Для этого нужно:

1. Нажать на значок в трее pgAdmin 4.
2. Выбрать «Настроить...».
3. Установить флажок с надписью «Фиксированный номер порта?».
4. Ввести желаемый номер порта в поле рядом с ним.

3) По умолчанию для работы PostgreSQL требуется разрешение порта 5432 по протоколу TCP/IP. [24](#)

Однако в некоторых случаях может быть необходим запуск PostgreSQL на другом порту, например, чтобы избежать конфликтов с другими сервисами или по соображениям безопасности. В таком случае нужно настроить файл postgresql.conf, который содержит настройки сервера PostgreSQL. [3](#)

Точный путь к файлу зависит от операционной системы и способа установки PostgreSQL. [3](#)

Кроме того, для аутентификации удалённого доступа к базам данных и пользователям можно использовать протокол md5 в файле pg_hba.conf.

3) Для работы HTTP (HyperText Transfer Protocol, протокол передачи гипертекста) требуется разрешить порт 80 (TCP). [34](#)

При этом для работы HTTP с поддержкой шифрования (HTTPS) используется порт 443 (TCP). [13](#)

Важно учитывать, что администратор сервера может настраивать используемые порты для запускаемых сетевых сервисов. Например, можно изменить номер порта, на котором работает веб-сервер, с 80 на 8080, но если пользователи не знают об этом, они не смогут подключиться к серверу.

4) Для работы протокола HTTPS обычно разрешают следующие порты и протоколы:

- Порт 443. Основной порт для HTTPS, обеспечивает шифрование связи веб-браузера с сервером с помощью сертификатов SSL или TLS. [15](#)
- Порт 8443. Альтернативный порт для HTTPS, часто используется для настройки безопасных соединений в конкретных приложениях или сервисах. [15](#)
- Порт 832. Предназначен для NETCONF для SOAP поверх HTTPS, обслуживает потребности настройки сети. 1
- Порт 5989. Зарезервирован для WBEM CIM-XML (HTTPS), служит стандартом для веб-управления предприятиями. 1
- Порт 8243. Связан с Synapse Non-Blocking HTTPS, предлагает неблокирующий подход к безопасной связи. 1
- Порт 16993. Выделен для Intel(R) AMT SOAP/HTTPS, обеспечивает безопасную связь в технологии активного управления Intel. 1
- Порт 20003. Предназначен для Commtact HTTPS, облегчает безопасную связь, специфичную для сервисов Commtact. 1

Кроме того, для аутентификации веб-сервера в HTTPS используются цифровые сертификаты, в частности SSL/TLS.

5) Для работы веб-интерфейса Zabbix по умолчанию необходимо разрешить следующие порты и протоколы:

- 80 — для HTTP-запросов (веб-интерфейс); [12](#)
- 443 — для HTTPS-запросов (веб-интерфейс); [12](#)
- 10051 — для сервера (используется с активными прокси/агентами); 1
- 10050 — для агента2; 1
- 10052 — для JavaGateway; 1
- 10053 — для WebService. 1

Эти порты нужно открыть в брандмауэре для обеспечения внешней связи с Zabbix. Обычно для исходящих TCP-соединений не требуются специальные настройки брандмауэра. 1

6) Для работы Django, в частности для запуска сервера разработки, требуется разрешить доступ к порту 8000. [13](#)

Информацию о других протоколах, которые необходимо разрешить для работы Django, найти не удалось.

При настройке Django-приложения часто используют такие сервисы, как Nginx, Gunicorn и другие, и для их работы могут потребоваться дополнительные настройки портов и протоколов, например, для Nginx может потребоваться разрешение стандартного для HTTP порта 80. [14](#)

Для более точной информации по настройке рекомендуется обратиться к специализированным инструкциям и руководствам, например, на сайтах dev.to, dvmn.org, timeweb.cloud.