Межсетевой экран Numa Edge

Руководство администратора

Краткое руководство по настройке

Листов 20

Санкт-Петербург
2021

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Краткое руководство по настройке
Версия документа	1.1.4
Обозначение документа	643.АМБН.00004-01 32 03
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, QSG
Официальная электронная документация по продукту	kb.numaedge.ru

1. ПОДКЛЮЧЕНИЕ NUMA EDGE

1.1. Настройки по умолчанию

1.1.1. Идентификационные и аутентификационные данные для Numa Edge

Для работы с интерфейсом устройства необходимо пройти процедуру аутентификации с использованием идентификатора учётной записи пользователя и пароля. По умолчанию в системе уже есть одна предварительно определённая учётная запись пользователя со следующими параметрами:

- идентификатор: **admin**
- пароль: **admin**

ПРИМЕЧАНИЕ Пароль для данной учетной записи необходимо изменить сразу же после начала использования системы.

По умолчанию удалённый доступ к Numa Edge разрешён только через управляющий порт Numa Edge. Расположение управляющего порта зависит от модели устройства.

1.1.2. Идентификационные и аутентификационные данные для доступа в БСВВ Numa BIOS

Для доступа к панели управления БСВВ Numa BIOS необходимо пройти процедуру аутентификации с использованием идентификатора учётной записи пользователя и пароля. По умолчанию в Numa BIOS уже есть одна предварительно определённая учётная запись пользователя со следующими параметрами:

- идентификатор: **admin**
- пароль: **Qwe123$**

ПРИМЕЧАНИЯ:

1. Пароль для данной учетной записи необходимо изменить сразу же после начала использования системы.
2. Рекомендуем запомнить/записать в недоступном для злоумышленника месте новые идентификационные и аутентификационные данные. При утрате логина/пароля восстановление этих данных невозможно, для возобновления работоспособности Изделия потребуется полная перепрошивка Изделия в сервисном центре ООО «НумаТех», при этом сохранность информации не гарантируется. Работы по перепрошивке Изделия осуществляются исключительно при наличии действующего сервисного сертификата на это устройство.
3. В случае ввода неправильного пароля более трёх раз административный пользователь будет заблокирован. Для возобновления работоспособности Изделия потребуется полная перепрошивка Изделия в сервисном центре ООО «НумаТех», при этом сохранность информации не гарантируется.
4. Предъявляются следующие требования к паролям:
   а) длина не менее 7 символов;
   б) буквы разного регистра;
   в) наличие цифр;
   г) наличие спецсимволов.
5. После установки нового пароля устройство будет перезагружено.

1.2. Получение доступа для управления

Для управления Numa Edge можно использовать интерфейс командной строки.

Интерфейс командной строки доступен и на управляющем порту, и при подключении через последовательный интерфейс.

1.2.1. Доступ через последовательный порт

При подключении через последовательный порт (RS-232) используются следующие параметры:

- скорость 115200 бит/с;
- без контроля чётности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bit).

1.2.2. Подключение к управляющему порту

Для получения удалённого доступа следует соединить порт Ethernet управляющего компьютера с управляющим портом Numa Edge при помощи кабеля (UTP категории 5), который входит в комплект поставки.

В качестве управляющего компьютера может быть использован любой персональный компьютер или ноутбук, оснащённый 10BASE-T/100BASE-T/1000BASE-T совместимым адаптером Ethernet.

Выбранный для связи с управляющим портом интерфейс Ethernet управляющего компьютера следует настроить на автоматическое получение адреса по DHCP, в результате чего устройством будет выдана конфигурация, достаточная для доступа к интерфейсу управления Numa Edge.

По умолчанию управляющий порт Numa Edge настроен на сеть 192.168.200.0/24 и имеет собственный адрес 192.168.200.1. Этот адрес должен использоваться для доступа к интерфейсам управления.

Для обеспечения безопасной передачи данных по протоколу SSH используется шифрование на основе стандартов ГОСТ Р 34.12-2018, ГОСТ Р 34.13-2018, а также аутентификация на основе стандарта ГОСТ 34.10—2012. По этой причине на управляющем компьютере должен использоваться клиент SSH, поддерживающий указанные криптографические алгоритмы.

1.3. Защита от сбоев при запуске

В Изделии Numa Edge присутствует механизм защиты от сбоев при запуске: соответствующий механизм призван выявить возможные неполадки Изделия на ранних стадиях эксплуатации. При старте Изделия базовая система ввода-вывода (БСВВ, BIOS) выставляет специализированное значение переменной («статус загрузки»), после чего управление передается операционной среде. При этом ожидается, что операционная среда при полностью успешном старте снимет установленное значение. Считается, что если статус был снят, то ПАК загрузился и работал в штатном режиме, иное значение «статуса загрузки», сигнализирует об ошибке загрузки ПАК. Значение рассматриваемой переменной (статуса загрузки) анализируется базовой системой ввода-вывода при каждом старте, и если значение сигнализирует об ошибке в процессе предыдущей загрузки Изделия - процесс текущей загрузки Изделия будет прерван, а на консольный порт Изделия будет выведено соответствующее сообщение об ошибке.

Перечень возможных сообщений БСВВ:

- «Ошибка контроля целостности Numa Edge».
- «Ошибка конфигурирования сервисов Numa Edge».
- «Ошибка запуска управляющего ПО: превышен лимит неудачных попыток запуска Numa Edge».

В случае возникновения соответствующего сообщения - необходимо изучить, что могло служить его причиной, а также перейти в панель управления БСВВ для вызова штатной загрузки Изделия.

ПРЕДУПРЕЖДЕНИЕ Если в процессе загрузки Изделия Numa Edge произойдет отключение электропитания, то значение соответствующего параметра («статуса загрузки») может быть не сброшено в соответствующее штатному режиму работы. Что в свою очередь вызовет срабатывание описываемого механизма защиты от сбоев. В целях предупреждения такого поведения рекомендуется подключать Изделие Numa Edge к сети электропитания через источники бесперебойного питания.

2. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

2.1. Интерфейс командной строки

2.1.1. Режимы команд

Интерфейс командной строки Numa Edge может находиться в двух режимах работы — эксплуатационном и настроечном:

- в эксплуатационном режиме обеспечивается доступ к командам отображения и очистки текущего состояния устройства, отображения конфигурации, включения или выключения отладки, настройки параметров терминалов, сохранения и загрузки состояния, а также перезапуска устройства;
- в настроечном режиме обеспечивается доступ к командам создания, изменения и удаления элементов конфигурации, а также к командам переходов по иерархии параметров.

По умолчанию, при входе в систему интерфейс находится в эксплуатационном режиме. Для перехода из эксплуатационного режима в режим настройки используется команда **configure**.

Для возврата из режима настройки в эксплуатационный режим используется команда **exit**. Переход в эксплуатационный режим при не зафиксированных изменениях в конфигурации не допускается, о чём устройство выдаёт соответствующее предупреждение. В этом случае, изменения необходимо либо применить с помощью команды **commit**, либо отменить с помощью команды discard (или выходить из режима настройки с помощью команды **exit discard**).

При выполнении команды **exit** в эксплуатационном режиме происходит выход из системы.

Когда устройство ожидает ввода команд, оно показывает соответствующее приглашение, которое также информирует пользователя о том, в каком режиме он работает с командной строкой, от имени какой учетной записи он работает и каково имя системы:

`admin@edge:-$`	Учётная запись: admin Имя системы: edge Режим интерфейса: эксплуатационный (символ «$»)
`[edit policy]` `admin@gate4#`	Учётная запись: admin Имя системы: gate4 Режим интерфейса: настроечный (символ «#») Ветвь конфигурации: policy

2.1.2. Автодополнение команд

В интерфейсе командной строки имеется функция автодополнения вводимых команд по первым введённым символам. Она задействуется клавиатурными комбинациями, описанными в таблице 1.

Таблица 1 – Клавиши автодополнения

Нажатые клавиши	**Результат**
<Tab>	Автодополнение команды: • если введённые символы можно дополнить однозначно, до единственной команды, то это и происходит; • если возможен более чем один вариант авто- дополнения, то система отображает список возможных последующих команд. При повторном нажатии клавиши <Tab> отображается справка интерфейса командной строки для списка возможных последующих команд.
?	При нажатии на клавишу с вопросительным знаком («?») также выполняется автодополнение команды. Для «обычного» ввода символа вопросительного знака, следует сначала нажать <Ctrl>+v, потом вопросительный знак.

3. КОНФИГУРАЦИЯ

3.1. Общие сведения по конфигурации

3.1.1. О возможности одновременного редактирования конфигурации

ПРЕДУПРЕЖДЕНИЕ Система конфигурирования Numa Edge не обеспечивает возможности одновременного редактирования конфигурации. К таким ситуациям относятся:

- одновременное редактирование конфигурации несколькими пользователями;
- одновременное редактирование конфигурации различными способами подключения (доступ к интерфейсу командной строки через последовательный порт, подключение по SSH, использование web-интерфейса).

В случаях, когда вероятна ситуация одновременной работы с конфигурацией, в первую очередь перед внесением изменений следует воспользоваться командой конфигурационного режима **show**. Если вы видите, что большая часть конфигурации устройства помечена на удаление, значит конфигурация была изменена в другой сессии. В таком случае предварительно следует выполнить команду **discard**.

3.1.2. Иерархия дерева конфигурации

Конфигурация устройства имеет древовидное строение и разделяется логически на узлы и атрибуты конфигурации. Атрибут конфигурации имеет вид атрибут значение, как в приведённом ниже примере:

```
cipher aes256-ctr
```

У узла конфигурации всегда есть закрытая пара фигурных скобок, содержимое которой может быть пусто, как в следующем примере:

```
service {
   https {
   }
}
```

или непусто, как в следующем примере:

```
ssh {
    address 192.168.1.1
}
```

3.1.3. Добавление параметров к конфигурации или изменение конфигурации

Добавление нового параметра производится в режиме настройки через создание атрибутов и узлов конфигурации командой **set**. Изменение существующего параметра выполняется тоже в режиме настройки с помощью команды **set**, как в приведённом ниже примере:

```
[edit]
admin@edge# set interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show**:

```
[edit]
admin@edge# show interfaces ethernet eth2
+address  192.168.1.100/24
```

Обратите внимание на знак «+» перед новым оператором. Он показывает, что оператор был добавлен к конфигурации, но изменение ещё не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit**.

Конфигурацию можно изменять, начиная с корня дерева конфигурации или использовать команду **edit** для перемещения к той ветви дерева, в которой надо выполнить изменения, а также команды **up** и **top** для возврата на верхние уровни.

При первой загрузке системы дерево конфигурации практически пусто, за исключением нескольких автоматически настроенных узлов. Вся функциональность системы настраивается через создание и изменение узлов и атрибутов конфигурации. Когда создаётся новый узел, для всех его атрибутов применяются значения по умолчанию.

3.1.4. Удаление параметров

Для удаления атрибута или целого узла в настройке служит команда **delete**, как в приведённом ниже примере:

```
[edit]
admin@edge# delete interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show**:

```
[edit]
admin@edge# show interfaces ethernet eth2
-address 192.168.1.100/24
```

Обратите внимание на знак «-» перед удалённым атрибутом. Он показывает, что атрибут был удалён из конфигурации, но изменение еще не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit**.

Некоторые узлы и атрибуты конфигурации являются обязательными, среди них есть такие, которые нельзя удалить, а есть имеющие значения по умолчанию, при удалении которых для них будет восстановлено это значение.

3.1.5. Фиксация изменений конфигурации

Изменения в конфигурации вступают в силу только после их фиксации командой **commit**:

```
[edit]
admin@edge# commit
```

При просмотре конфигурации имеющиеся незафиксированные изменения помечаются знаком «+» (в случае добавления/правки) или «-» (в случае удаления). При фиксации изменений знаки удаляются, как в приведённом ниже примере:

```
[edit]
admin@edge# show interfaces ethernet eth2
-address 192.168.1.100/24
[edit]
admin@edge# commit
[edit]
admin@edge# show interfaces ethernet eth2
[edit]
admin@edge#
```

Изменения фиксируются в текущей (активной) конфигурации. Для того чтобы полученная конфигурация использовалась после перезагрузки устройства она должна быть сохранена в файл командой **save**, см. раздел «Сохранение конфигурации в файл».

3.1.6. Отмена изменений в конфигурации

Выйти из режима настройки при наличии незафиксированных изменений невозможно: необходимо либо фиксировать изменения, либо отказаться от них. Если фиксировать изменения не нужно, можно отменить их с помощью команды **exit discard**:

```
[edit]
admin@edge# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
[edit]
admin@edge# exit discard
admin@edge01:~$
```

3.1.7. Сохранение конфигурации в файл

Действующую в данный момент конфигурацию можно сохранить в файл при помощи команды **save** в режиме настройки. По умолчанию, конфигурация сохраняется в файл config.boot в стандартном каталоге конфигурации, которым является /etc/config:

```
[edit]
admin@edge# save
Запись конфигурации в '/etc/config/config.boot'...
Готово
```

При включении питания устройство загружает конфигурацию именно из файла /etc/config/config.boot, поэтому после успешной настройки всех необходимых сервисов важно сохранить текущую конфигурацию в этот файл.

Можно сохранить конфигурацию под другим именем, указав другое имя файла:

```
[edit]
admin@edge# save testconfig
Запись конфигурации в  '/etc/config/testconfig'...
Готово
```

Для сохранения файла конфигурации можно указать и другой каталог, отличный от стандартного /etc/config. Сохранять можно на жесткий диск, карту CF или USB-накопитель, включив точку монтирования носителя в путь. Также поддерживается сохранение файла на сервера FTP, TFTP. Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует смонтировать командой **flash mount** в эксплуатационном режиме.

Обратите внимание, что команда **save** записывает только актуальную конфигурацию.

3.1.8. Загрузка конфигурации

Для загрузки ранее сохранённой конфигурации используется команда **load** в режиме настройки. По умолчанию система считывает файл из стандартного каталога конфигурации — /etc/config:

```
[edit]
admin@edge# load testconfig
Loading config file /etc/config/testconfig...
```

```
Done
```

Загруженная конфигурация автоматически применяется и становится активной конфигурацией.

Для загрузки файла конфигурации можно указать и другой каталог, отличный от стандартного /etc/config. Загружать конфигурацию можно с жесткого диска карт CF или USB-накопителей, включив точку монтирования носителя в путь. Также поддерживается загрузка конфигурации с серверов FTP, TFTP или HTTP.

В таблице 2 приведены поддерживаемые устройством пути для сохранения или загрузки файла конфигурации:

Таблица 2 – Способы указания местоположения файла конфигурации

Местоположение	**Способ указания**
Абсолютный путь	Используется стандартный способ указания файла в UNIX
Относительный путь	Указывается имя файла относительно стандартного каталога /etc/config.
Сервер TFTP	Используется следующий синтаксис для имени файла: tftp://ip-адрес/файл_конфигурации, где ip-адрес это IP-адрес сервера TFTP, а файл_конфигурации это файл конфигурации, включая путь относительно корневого каталога TFTP.
Сервер FTP	Используется следующий синтаксис для имени файла: ftp://ip-адрес/файл_конфигурации, где ip-адрес — это IP-адрес сервера FTP, а файл_конфигурации — это файл конфигурации, включая путь. При использовании FTP будет выдан запрос на ввод имени учётной записи на сервере FTP и её пароля.
Сервер HTTP (только для загрузки конфигурации)	Используется следующий синтаксис для имени файла: http://ip-адрес/файл_конфигурации, где ip-адрес это IP-адрес сервера HTTP, а файл_конфигурации это файл конфигурации, включая путь.

3.2. Пример. Базовая конфигурация

В этом разделе приведён пример начальной настройки системы. Для доступа к интерфейсу командной строки используется протокол SSH. Работа ведётся от имени учетной записи, определённой по умолчанию: идентификатор пользователя — admin, пароль — admin.

3.2.1. Переход в режим настройки

После входа в систему мы оказываемся в эксплуатационном режиме, являющимся режимом по умолчанию:

```
Last login: Mon Sep  7 13:48:00 MSK 2020 from  192.168.200.100
admin@edge:-$
```

Для настройки системы необходимо перейти в режим настройки:

```
admin@edge:-$ configure
[edit]
admin@edge#
```

3.2.2. Установка имени системы

По умолчанию системе присвоено имя edge. При необходимости это значение можно изменить:

```
[edit]
admin@edge# set system host-name gate
[edit]
```

```
admin@edge# commit
```

Вид приглашения, соответствующий новому имени системы, появится при следующем входе в систему.

3.2.3. Установка имени домена

В дополнение к изменению имени системы, может потребоваться изменить имя домена:

```
[edit]
admin@edge# set system dns domain-name numatech.ru
[edit]
admin@edge# commit
```

3.2.4. Изменение пароля

По умолчанию в системе есть одна предварительно определённая учётная запись пользователя:

- идентификатор пользователя: **admin;**
- пароль по умолчанию: **admin.**

Пароль для данной учётной записи необходимо изменить сразу же после начала использования системы:

```
[edit]
admin@edge# set system login user admin authentication plaintext-password
'bt12plo%14P'
[edit]
admin@edge# commit
```

3.2.5. Настройка интерфейсов

Тип и номер изменяемого интерфейса зависят от используемого устройства и топологии сети. Однако, практически при любой топологии сети требуется настройка по крайней мере одного интерфейса Ethernet. В этом примере приведена настройка интерфейса eth1 в качестве интерфейса, к которому подключён внешний сегмент сети:

```
[edit]
admin@edge# set interfaces ethernet eth1 address 203.0.113.10/24
[edit]
admin@edge# commit
```

В том случае, когда провайдер предоставляет сетевые настройки по протоколу DHCP, следует использовать команду **set interfaces ethernet eth1 address dhcp**.

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show interfaces ethernet
eth1 {
    address 203.0.113.10/24
}
```

3.2.6. Настройка маршрута по умолчанию

Получателем трафика, для которого Numa Edge не может определить маршрут исходя из собственных таблиц маршрутизации, является другое внешнее устройство, называемое

маршрутизатором по умолчанию (а путь отправки такого трафика называется маршрутом по умолчанию). Адрес маршрутизатора по умолчанию указывается следующим образом:

```
[edit]
admin@edge# set system gateway-address 203.0.113.100
[edit]
admin@edge# commit
```

3.3. Пример. Интернет-шлюз

Рассматриваемая в этом примере конфигурация предполагает следующее:

- настройка маршрутизации сетевого трафика между локальной сетью (LAN) и интернетом;
- возможность получения доступа к Numa Edge по протоколу SSH из внутренней сети;
- назначение адресов устройствам во внутренней локальной сети динамически, по протоколу DHCP;
- использование ретрансляции DNS для устройств во внутренней локальной сети;
- использование NAT для преобразования внутренних адресов в один внешний адрес;
- настройка межсетевого экрана для предотвращения доступа к системе из внешнего сегмента сети (интернета).

В данном примере приведена настройка двух интерфейсов Ethernet, к одному из которых (eth1) подключён внешний сегмент сети (WAN), а к другому (eth2) подключён локальный сегмент сети (LAN), как показано на рисунке 1.

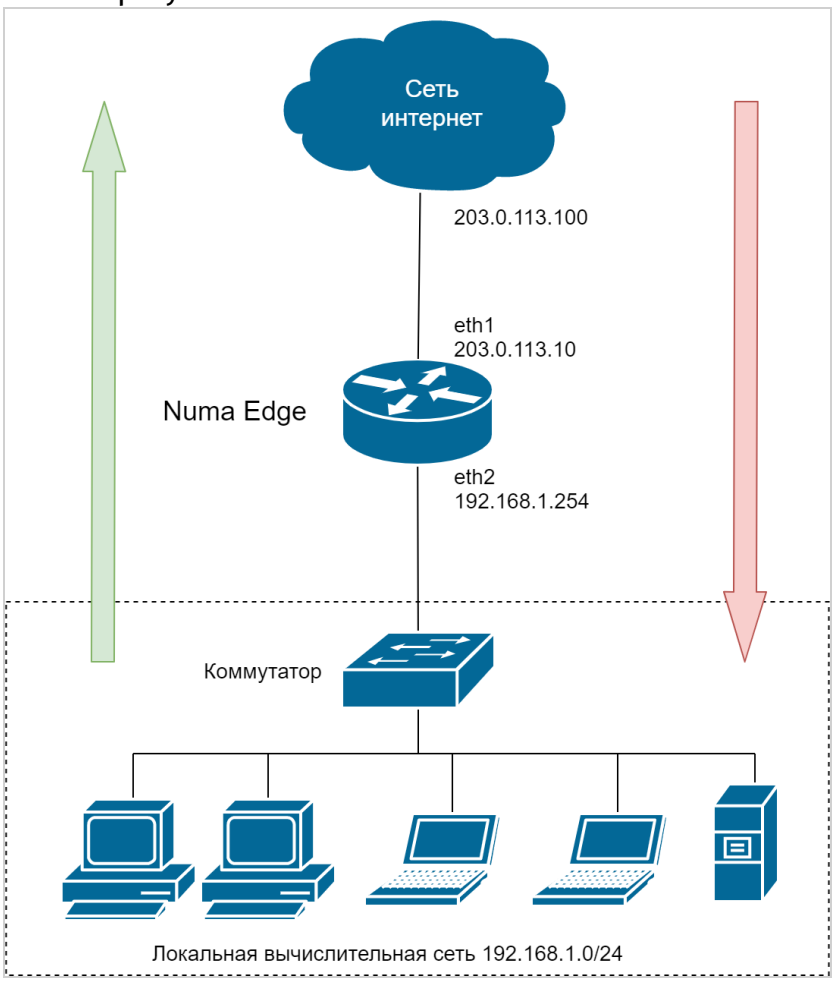

Рисунок 1 – Интернет-шлюз

В этом примере также предполагается, что уже выполнена настройка из предыдущего примера.

3.3.1. Настройка интерфейсов

В предыдущем примере был настроен внешний интерфейс eth1. Для того, чтобы Numa Edge функционировал в качестве интернет-шлюза, в системе необходимо настроить ещё один интерфейс, к которому будет подключён локальный сегмент сети (LAN). В нашем случае используется интерфейс eth2:

```
[edit]
admin@edge# set interfaces ethernet eth2 address 192.168.1.254/24
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show interfaces ethernet
    eth1 {
        address 203.0.113.10/24
    }
    eth2 {
        address 192.168.1.254/24
    }
```

3.3.2. Включение доступа по протоколу SSH

По умолчанию доступ к Numa Edge по протоколу SSH разрешён только на управляющем интерфейсе. Доступ из локальной сети включается следующей командой:

```
[edit]
admin@edge# set service ssh address 192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service ssh
   address 192.168.1.254 {
   }
   cipher kuznechik-ofb
   hmac hmac-stribog-256
   hmac hmac-stribog-512
   key-exchange-algo ecdh-gost2012-256-cpa
   client-alive-timeout 1800
   disable-password-authentication false
```

3.3.3. Настройка сервера DHCP

Протокол динамической настройки системы (Dynamic Host Configuration Protocol, DHCP) обеспечивает динамическое назначение IP-адресов и других сведений о настройке системам указанного сегмента сети. В нашем примере сервер DHCP обеспечивает динамическое назначение IP-адресов компьютерам в локальной сети (LAN).

В настройке сервера DHCP необходимо определить перечень (блок/пул) адресов, которые будут выдаваться клиентам в локальной сети (192.168.1.100—192.168.1.199). В качестве маршрутизатора по умолчанию и сервера доменных имен будет указываться адрес внутреннего интерфейса (eth2) Numa Edge:

```
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 start 192.168.1.100
stop 192.168.1.199
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 default-router
192.168.1.254
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 dns-server
192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@edge# show service dhcp-server
   subnet 192.168.1.0/24 {
        default-router 192.168.1.254
        start 192.168.1.100 {
            stop 192.168.1.199
        }
   }
```

3.3.4. Настройка DNS

3.3.4.1. Системный сервер DNS

Настраиваемый системный сервер DNS будет использоваться самим Numa Edge и всеми его сервисами для разрешения имён. Обычно указывается предоставленный провайдером сервер DNS. В отсутствие настройки конкретного используемого сервера DNS будут использоваться сервера, получаемые с помощью протокола DHCP, либо полученные через туннели PPPoE, PPTP, OpenVPN и т.п. Статическая настройка использования конкретного сервера выполняется следующим образом:

```
[edit]
admin@edge# set system dns name-server 203.0.113.100
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show system dns
   domain-name numatech.ru
   name-server 203.0.113.100 {
   }
```

3.3.4.2. Сервис ретрансляции DNS

Сервис ретрансляции DNS позволяет клиентам локальной сети использовать Numa Edge для разрешения имён посредством протокола DNS. По умолчанию, сам сервис использует доступные системные сервера DNS, а настройка доступа требует указания интерфейса. В данном примере необходимо указать внутренний интерфейс (eth2):

```
[edit]
admin@edge# set service dns forwarding listen-on address 192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service dns forwarding
   listen-on {
       address 192.168.1.254
   }
```

3.3.5. Настройка NAT

Интернет-шлюз должен отправлять исходящий сетевой трафик из локальной сети через внешний интерфейс и заменять внутренние адреса на внешний общедоступный адрес. Для этого необходимо определить правило NAT.

Определим правило, обеспечивающее прохождение трафика из внутренней подсети 192.168.1.0/24 в интернет через интерфейс eth1 и заменяющее внутренние адреса на внешний адрес интерфейса eth1:

```
[edit]
admin@edge# set service nat ipv4 rule 1 source address 192.168.1.0/24
[edit]
admin@edge# set service nat ipv4 rule 1 outbound-interface eth1
[edit]
admin@edge# set service nat ipv4 rule 1 type masquerade
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service nat ipv4
   rule 1 {
       outbound-interface eth1
```

```
        source {
            address 192.168.1.0/24
        }
        type masquerade
    }
```

3.3.6. Настройка межсетевого экрана (МЭ)

При настройках по умолчанию Numa Edge никак не ограничивает прохождение сетевого трафика. Передача трафика через интерфейс разрешена до тех пор, пока к интерфейсу не будет применено правило МЭ. В данном примере интернет-шлюз должен разрешать доступ к интернету устройствам из локальной сети и собственным службам, но необходимо блокировать трафик, инициированный источниками из внешнего сегмента сети.

В общем случае, для настройки правил МЭ на интерфейсе необходимо сделать следующее:

- определить поименованные наборы правил МЭ (т.н. экземпляры МЭ), каждый из которых может содержать одно или более правил;
- применить необходимые экземпляры МЭ к интерфейсу. Экземпляр МЭ может фильтровать пакеты одного из следующих направлений:
  - **in** (входящий). Если применить экземпляр с использованием ключевого слова **in,** то межсетевой экран будет фильтровать пакеты, входящие в интерфейс и транзитно проходящие через устройство;
  - **out** (исходящий). Если применить экземпляр с использованием ключевого слова **out,** то межсетевой экран будет фильтровать транзитные пакеты, проходящие через устройство, и покидающие её через указанный интерфейс;
  - **local** (локальный). Если применить экземпляр с использованием ключевого слова **local,** то межсетевой фильтр будет фильтровать пакеты, предназначенные самому устройству (не транзитные).

При этом для одного направления трафика может быть применён только один экземпляр МЭ.

3.3.6.1. Определение экземпляра МЭ

Создание правила для пропуска в локальный сегмент сети только ответного трафика, порождённого исходящим трафиком этого сегмента (т.е. установленными из LAN наружу соединениями и связанным с ними трафиком):

```
[edit]
admin@edge# set filter ALLOW_ESTABLISHED
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10 state established enable
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10 state related enable
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED rule 10 action accept
```

```
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED rule 10 match filter
ALLOW_ESTABLISHED
[edit]
admin@edge# commit
```

3.3.6.2. Применение экземпляра МЭ к интерфейсу

Применение набора правил ALLOW_ESTABLISHED к сетевому трафику, приходящему на интерфейс:

```
[edit]
admin@edge# set interfaces ethernet eth1 policy in firewall ALLOW_ESTABLISHED
[edit]
admin@edge# set interfaces ethernet eth1 policy local firewall
ALLOW_ESTABLISHED
```

Если в разделе «Настройка интерфейсов» использовалась настройка внешнего интерфейса по DHCP, применение МЭ к направлению local сделает невозможной конфигурацию интерфейса по DHCP, следует либо не применять соответствующую настройку, либо добавить разрешительные правила для протокола DHCP в МЭ.

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show policy firewall
   ALLOW_ESTABLISHED {
       rule 10 {
           action accept
           match {
               filter ALLOW_ESTABLISHED
           }
       }
   }
[edit]
admin@edge# show filter
   ALLOW_ESTABLISHED {
       rule 10 {
           state {
               established enable
               related enable
           }
       }
   }
[edit]
admin@edge#
```

Просмотр параметров интерфейса:

```
admin@edge# show interfaces
   ethernet eth1 {
       address 203.0.113.21/24
       policy {
           in {
               firewall ALLOW_ESTABLISHED
           }
           local {
               firewall ALLOW_ESTABLISHED
           }
       }
   }
   ethernet eth2 {
       address 192.168.1.254/24
   }
```

4. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для создания заявок и переписки с сервисной службой существует портал, доступный по адресу https://support.numatech.ru/. Взаимодействовать с сервисной службой можно также через почту, заявки автоматически создаются для писем, направленных на адрес support@numatech.ru.

Для ускорения обработки заявок, рекомендуется сопровождать их выводом команды эксплуатационного режима **show tech-support**. Сохранить вывод **show tech-support** на флэш-накопитель вы можете следующим образом:

Подключите флэш-накопитель к устройству (накопитель должен быть форматирован в файловую систему FAT или FAT32);

Выполните следующие эксплуатационные команды:

```
admin@edge:-$flash mount
admin@edge:-$show tech-support save /media/hdd/tech
admin@edge:-$flash umount
```

Извлеките флэш-накопитель из устройства.

В корневом каталоге будет находиться файл с именем tech.[имя_устройства].tech-support.[текущая_дата].gz, который и необходимо отправить специалистам сервисной службы.