Техническая документация

плата MC-03 как Session Border Controller (SBC)

1. Введение

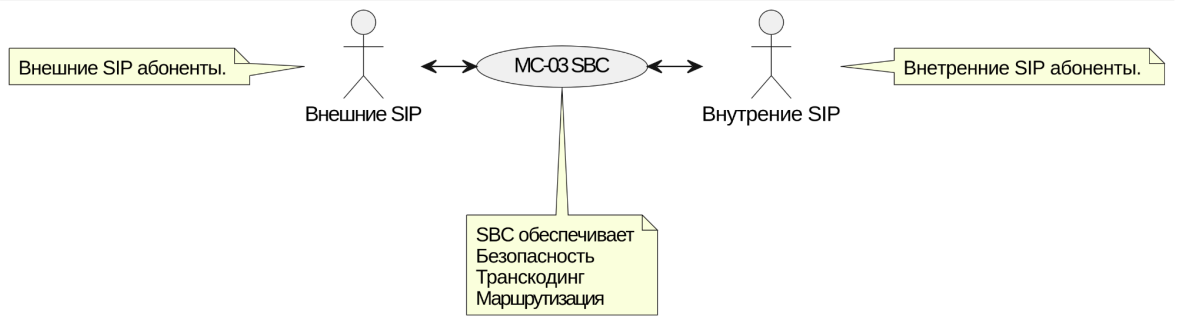
1.1. Назначение

Данный документ описывает конфигурацию и использование платы MC-03 в качестве SBC для защиты SIP-инфраструктуры, маршрутизации вызовов и обеспечения межсетевого взаимодействия.

1.2. Возможности MC-03 как SBC

- **Гибкость**: Полный контроль над обработкой вызовов
- **Интеграция**: Совместимость с различными VoIP-платформами

2. Архитектура решения



3. Установка и базовая настройка

3.1. Установка образа SBC

Скачать последнюю версию образа из репозитория https://repo.mvtel.by/MC-03/updates/sbc/ .
Установить образ на плату MC-03 согласно инструкции по установке.

3.2. Базовая конфигурация

```
# Скопировать конфигурацию по умолчанию
cp -R /etc/freeswitch/ /persist/etc/freeswitch

# Структура каталогов конфигурации
/persist/etc/freeswitch/
├── autoload_configs/
├── sip_profiles/
├── dialplan/
└── directory/
```

3.3. Конфигурация IP адресов

/persist/etc/network/interfaces

```
auto lo
iface lo inet loopback

# Внутренний интерфейс
auto eth0
iface eth0 inet static
  address 192.168.15.50
  netmask 255.255.255.0
  gateway 192.168.15.2

# Внешний интерфейс в 100 vlan
auto eth0.100
iface eth0.100 inet static
  address 10.8.1.2
  netmask 255.255.255.0
  gateway 10.8.1.1
  vlan-raw-device eth0
```

3.5 Запрет маршрутизации

Проверяем разрешена ли маршрутизация пакетов между внутренними интерфейсами

```
# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0

##Если значение 0, значит маршрутизация запрещена (значение по умолчанию)
## Если значение 1, то запретить маршрутизацию

# sysctl net.ipv4.ip_forward=1
```

4. Конфигурация SIP-профилей

4.1. Внешний профиль (external)

/persist/etc/sip_profiles/external.xml

```
<profile name="external">
```

```
  <settings>
      <!-- Базовые настройки -->
      <param name="listen-ip" value="0.0.0.0"/>
      <param name="listen-port" value="5080"/>
      <param name="apply-nat-acl" value="rfc1918.auto"/>
      <param name="apply-inbound-acl" value="external_acl"/>

      <!-- Безопасность -->
      <param name="accept-blind-auth" value="false"/>
      <param name="inbound-reg-force-matching-username" value="true"/>

      <!-- RTP настройки -->
      <param name="rtp-ip" value="$${local_ip_v4}"/>
      <param name="sip-ip" value="$${local_ip_v4}"/>
      <param name="ext-rtp-ip" value="$${external_rtp_ip}"/>
      <param name="ext-sip-ip" value="$${external_sip_ip}"/>

      <!-- Тайм-ауты -->
      <param name="enable-timer" value="true"/>
      <param name="session-timeout" value="1800"/>
  </settings>
</profile>
```

4.2. Внутренний профиль (internal)

/persist/etc/freeswitch/sip_profiles/internal.xml

```
<profile name="internal">
  <settings>
      <param name="listen-ip" value="$${local_ip_v4}"/>
      <param name="listen-port" value="5060"/>
      <param name="apply-inbound-acl" value="internal_acl"/>
      <param name="accept-blind-reg" value="false"/>
      <param name="require-register" value="true"/>
  </settings>
```

5. Настройка ACL (Access Control Lists)

5.1. Конфигурация ACL

/persist/etc/freeswitch/autoload_configs/acl.conf.xml

```
<configuration name="acl.conf" description="Network Lists">
```

```
  <network-lists>
      <list name="external_acl" default="deny">
      <node type="allow" cidr="sip-provider-ip/32"/>  <!--
SIP-провайдер -->
      </list>

      <list name="internal_acl" default="deny">
      <node type="allow" cidr="192.168.1.0/24"/>  <!-- Внутренняя сеть
-->
      </list>
  </network-lists>
</configuration>
```

6. Диалплан для маршрутизации вызовов

6.1. Входящие вызовы от провайдеров

/persist/etc/freeswitch/dialplan/default.xml

```
<context name="public">
  <extension name="incoming_from_provider">
      <condition field="destination_number" expression="^(\d+)$">
      <action application="log" data="INFO Incoming call from
Provider1 to ${destination_number}"/>

      <!-- Маршрутизация на внутреннюю АТС -->
      <action application="bridge"
data="sofia/internal/${destination_number}@internal-pbx-ip"/>
      </condition>
  </extension>
</context>
```

6.2. Исходящие вызовы через провайдеров

```
<context name="default">
  <extension name="outbound_routing">
      <condition field="destination_number" expression="^0(\d+)$">
      <!-- Маршрутизация через Provider1 -->
      <action application="set"
data="effective_caller_id_number=your_number"/>
      <action application="bridge"
data="sofia/external/${destination_number}@provider1-gateway"/>
```

```
      </condition>

      <condition field="destination_number" expression="^80(\d+)$">
      <!-- Международные вызовы через Provider2 -->
      <action application="bridge"
data="sofia/external/${destination_number}@provider2-gateway"/>
      </condition>
  </extension>
</context>
```

7. Настройка безопасности

7.1. Fail2Ban интеграция

/etc/fail2ban/jail.local

```
[freeswitch]
enabled = true
port = 5060,5080
filter = freeswitch
logpath = /var/log/freeswitch/freeswitch.log
maxretry = 3
bantime = 3600
```

7.2. IPtables правила

```
# Базовые правила firewall
iptables -A INPUT -p udp --dport 5060:5080 -j ACCEPT
iptables -A INPUT -p udp --dport 16384:32768 -j ACCEPT  # RTP порты
# Разрешить ssh на внутренем интерфейсе
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j
ACCEPT

# Запретить все остальное
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

8. Мониторинг и логирование

8.1. Настройка логов

/persist/etc/freeswitch/autoload_configs/switch.conf.xml

```
<settings>
  <param name="loglevel" value="INFO"/>
  <param name="console-log-level" value="INFO"/>
  <param name="sip-capture" value="no"/>
</settings>
```

9. Транскодинг и обработка медиа

9.1. Настройка кодеков

/persist/etc/freeswitch/autoload_configs/switch.conf.xml

```
<configuration name="switch.conf">
  <settings>
      <param name="global-codec-prefs"
value="PCMA,PCMU,G711,G729,GSM"/>
      <param name="outbound-codec-prefs" value="PCMA,PCMU,G711,G729"/>
  </settings>
</configuration>
```

10. Обработка NAT

10.1. Настройка для работы за NAT

```
<!-- В external.xml профиле -->
<param name="ext-rtp-ip" value="ВАШ_PUBLIC_IP"/>
<param name="ext-sip-ip" value="ВАШ_PUBLIC_IP"/>
<param name="NDLB-received-in-nat-reg-contact" value="true"/>
<param name="NDLB-force-rport" value="true"/>
```

11. Резервное копирование и восстановление

11.1. Скрипт бэкапа

```
#!/bin/bash
# backup-freeswitch.sh

DATE=$(date +%Y%m%d)
```

```
BACKUP_DIR="/tmp/backup/freeswitch/$DATE"

mkdir -p $BACKUP_DIR
cp -r /persist/etc/freeswitch/ $BACKUP_DIR/
tar -czf $BACKUP_DIR/freeswitch-backup-$DATE.tar.gz $BACKUP_DIR
```

12. Заключение

Данная конфигурация позволяет использовать МС-03 в качестве полнофункционального SBC с поддержкой:
- Межсетевого экранирования
- Маршрутизации вызовов
- Транскодинга кодеков
- Мониторинга и безопасности

Конфигурация должна быть адаптирована под конкретные требования заказчика.

В особых случаях, когда внешнее подключение производится к оператору связи, может понадобится нормализация заголовков SIP сообщений под конкретные требования оператора. В таком случае образ SBC платы МС-03 может быть дополнен SIP прокси сервером для выполнения нормализации сообщений.