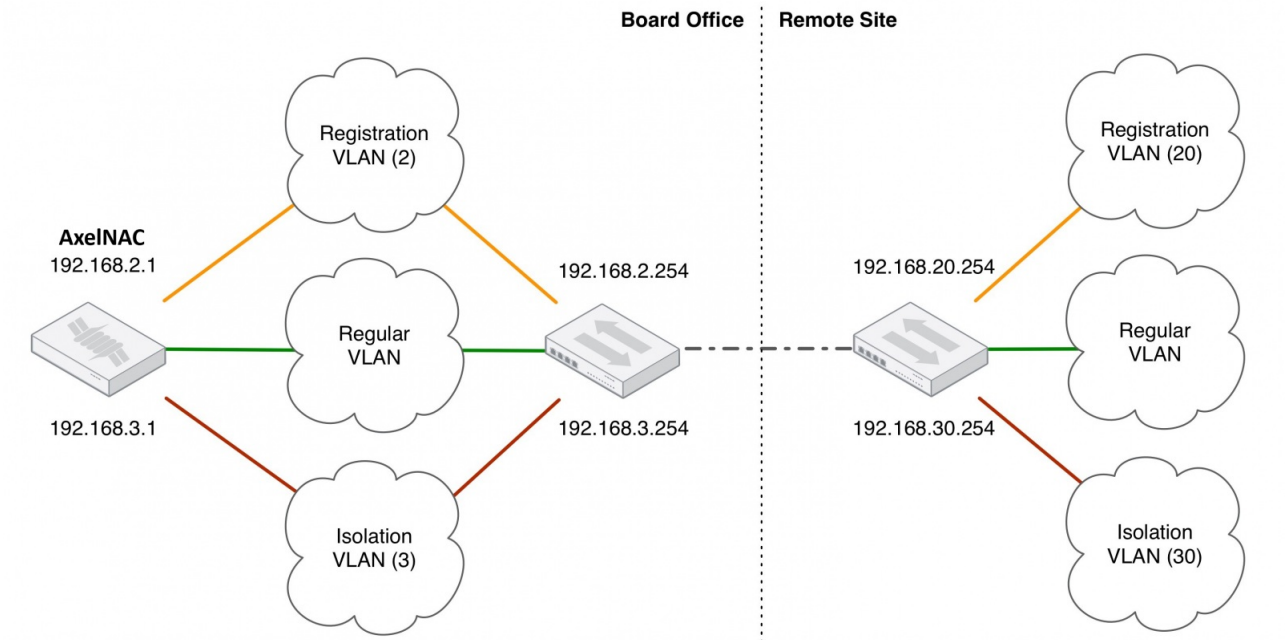
Маршрутизированные сети

Настройка AxelNAC необходима в тех случаях, если сети изоляции и регистрации недоступны локально в сети (Layer 2), но вместо этого маршрутизируются на сервер AxelNAC. В таких маршрутизируемых сетях AxelNAC может обеспечить работу DHCP и DNS:



	Registration VLAN	Isolation VLAN	Isolation VLAN	Registration VLAN
VLAN ID	2	3	30	20
Network	192.168.2.0/24	192.168.3.0/24	192.168.30.0/24	192.168.20.0/24
Gateway	192.168.2.254	192.168.3.254	192.168.30.254	192.168.20.254
DHCP	192.168.2.1	192.168.3.1	192.168.3.1	192.168.2.1
DNS	192.168.2.1	192.168.3.1	192.168.3.1	192.168.2.1
AxelNAC	192.168.2.1	192.168.3.1		

Для работы службы **dhcpd** убедитесь, что DHCP-запросы клиентов правильно пересылаются (IP Hepler на удаленных маршрутизаторах) на сервер AxelNAC. Для приведенной выше архитектуры сети в конфигурацию будут включены только локальные интерфейсы **Registration** и **Isolation**:

```
[interface eth0.2]
enforcement=vlan
ip=192.168.2.1
type=internal
mask=255.255.255.0

[interface eth0.3]
enforcement=vlan
ip=192.168.3.1
type=internal
mask=255.255.255.0
```

AxelNAC не запустится до тех пор, пока не будет обнаружен хотя бы один «внутренний» интерфейс. Поэтому локальные сети регистрации и изоляции должны быть созданы, даже если они не нужны. Демон **dhcpd** прослушивает только «внутренние» интерфейсы, поэтому для удаленных подсетей регистрации и изоляции должны быть настроен DHCP Helper, указывающий на эти конкретные IP-адреса.

Укажите маршрутизируемые сети в AxelNAC через веб-интерфейс в разделе **Конфигурация → Сетевое взаимодействие → Сети**.

Для вступления изменений в силу, перезапустите службу **keepalived**.

DHCP-клиенты в сетях регистрации и изоляции получают в качестве DNS-сервера IP-адрес сервера AxelNAC, а затем DNS-ответы подменяются для принудительной отправки клиентов через портал. Однако клиенты могут вручную настроить свои параметры DNS, чтобы избежать открытия портала. Для этого примените ACL на ближайшем к клиентам маршрутизаторе доступа, разрешив доступ только к серверу AxelNAC и локальному широковещательному трафику DHCP.

Пример ACL для удаленной сети регистрации VLAN 20:

```
ip access-list extended ANAC_REGISTRATION
```

```
permit ip any host 192.168.2.1
permit udp any any eq 67
deny ip any any log
interface vlan 20
ip address 192.168.20.254 255.255.255.0
ip helper-address 192.168.2.1
ip access-group ANAC_REGISTRATION in
```

Если пограничные коммутаторы поддерживают функцию изоляции **vlan-isolation**, ACL также можно применить и к ним. Преимущество этого способа заключается в том, что компьютеры, находящиеся в VLAN изоляции, не могут атаковать друг друга.

ID статьи: 623
Последнее обновление: 3 окт., 2024
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Расширенная конфигурация сети -> Маршрутизированные сети
https://docs.axel.pro/entry/623/