

Основы построения защищенных сетей ViPNet 4го поколения.

Игорь Виноходов

Немного истории

ViPNet Администратор 4

- 2013г
- 4.0 → 4.4.1 → 4.6.10

ViPNet Coordinator HW 4

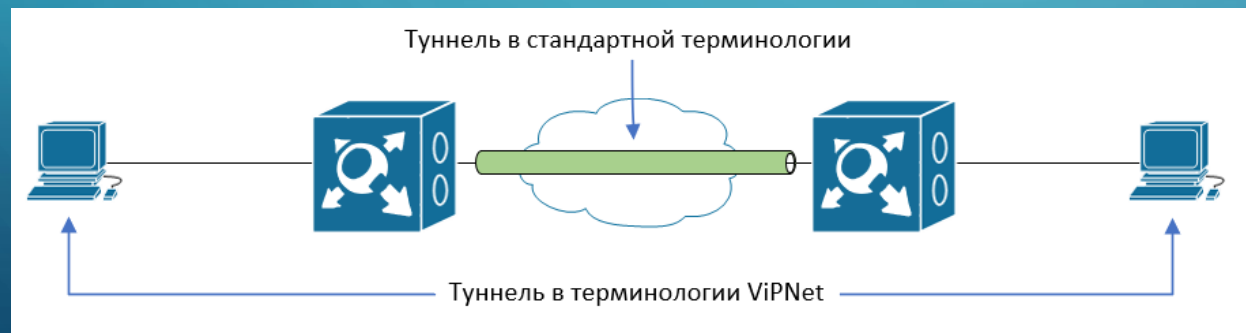
- 2014г
- 4.0 → 4.1.1 → 4.3.2(+VA) → 4.5.2

EOS 2024 или 2025?



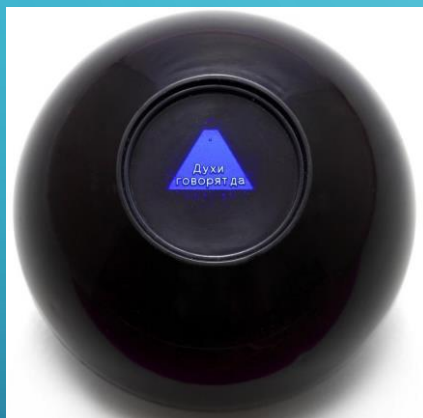
Терминология

- Coordinator
- Конверт
- Справочники
- Транспортный модуль(MFTP)
- Туннель
- IPir
- Связи



Основные причины недоступности узлов:

- Отсутствие сетевой связности
- Неверный вариант настройки работы через МЭ
- Отсутствие маршрута по умолчанию
- Расхождение во времени между узлами
- Нет ключей шифрования/неверные ключи



```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= off
registerbroadcast= off
omittcpclientport= off
registerevents= on
```

Системные настройки

Дата и время Управление устройством SNMP SSH Журналы

🔍 Поиск... Установить на всех интерфейсах ▾

Интерфейс	Регистрировать все пакеты	Регистрировать заблокированные
eth0	<input checked="" type="radio"/>	<input type="radio"/>
eth1	<input type="radio"/>	<input checked="" type="radio"/>
eth2	<input checked="" type="radio"/>	<input checked="" type="radio"/>
eth3	<input type="radio"/>	<input checked="" type="radio"/>

Транспортный модуль



Режимы работы транспортного модуля:

- Через сервер
- MFTR
- POP3/SMTP
- Локальный
- Отключен



Причины недоставки конверта:

- Неверный режим работы транспортного модуля
- Нет связи между узлами в цепочке доставки
- Проблемы с MTU (overhead)
- Большая очередь конвертов
- Не запущена служба транспортного модуля

Виртуальная адресация

[id]
tunnel= 1.1.1.1-1.1.1.5 to 12.0.0.1-12.0.0.5

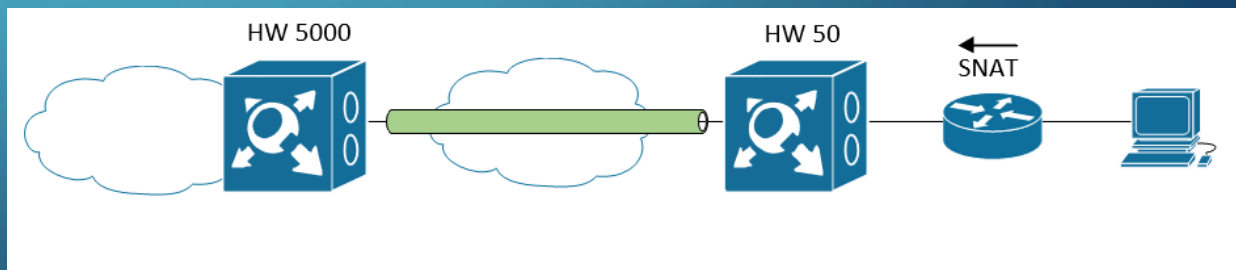
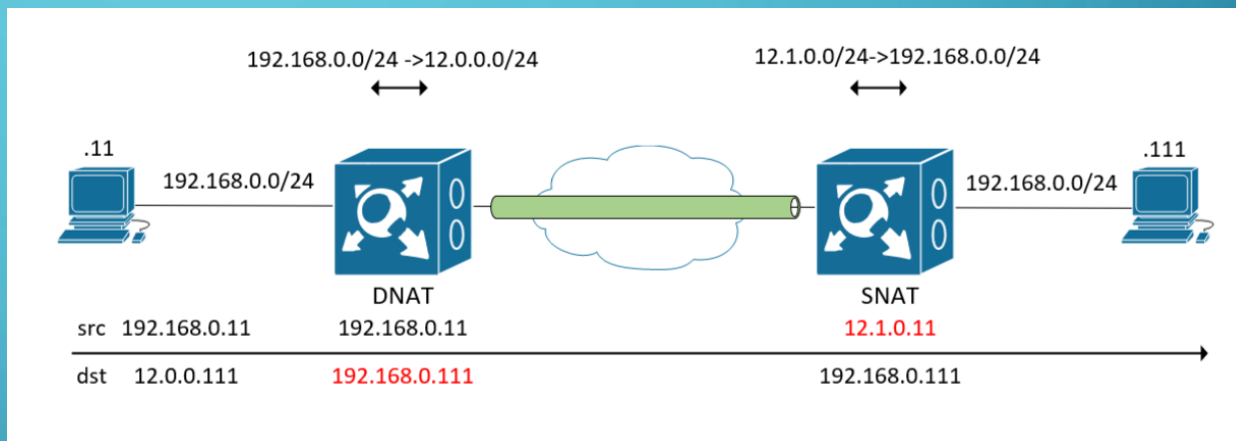
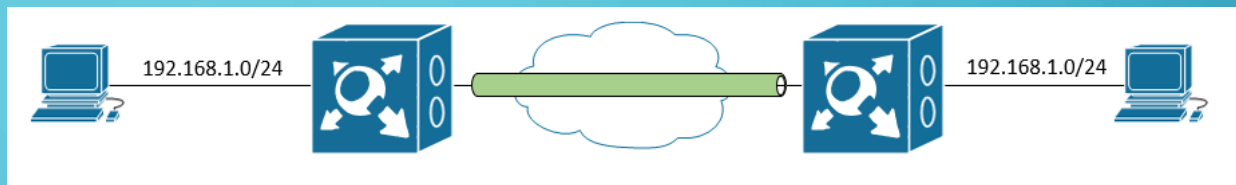
[visibility]
tunneldefault= virtual
tunnel_local_networks= on

[id]
tunnelvisibility= virtual

[id]
usetunnel= off
exclude_from_tunnels= 1.1.1.1-1.1.1.5

[misc]
tunnel_virt_assignment= manual

TUN адрес 7.XX.YY.7
ID: 0x04D2162E — 7.22.46.7



Диагностика

iplirdiag -s ipsettings --node-info <node id>

iplirdiag -s ipsettings --v-tun-table

iplirdiag -s ipsettings --v-table

```
sh-4.4# iplirdiag -s ipsettings --node-info A08A000A
Node row
node: A08A000A
proxyType: StaticwithoutFixIpAddress
visibility: Real
methodIpAddress: None
numRealIps: 4
numTunnelingIps: 6
firstVirtualIp: 0.0.0.0
firewallIp: 10.1.1.34
accessUdpPort: 55777
proxyId: FFFFFFFD
forwardId: A08A000A
forwardIdExist: 1
incType: IncapsForceRealIp (0x400)
properties: SupportGostOfb Coordinator (0x400004)
timeout: 0
timestamp: 0
lastAdapterNumber: -1
hasTunnelLicense: 1
Internet Gateway mode: No

Request node access point for A08A000A return errorCode=18

The ip address table for node A08A000A(rows 4):
Real visibility
10.1.1.11 10.1.1.11
10.1.1.34 10.1.1.34
10.1.1.52.2 10.1.1.52.2
172.1.1.1 172.1.1.1

The tunneling ip address table for node 378A000A(rows 6):
Begin real End real Begin visibility End visibility
10.1.1.11 10.1.1.11 10.1.1.11 10.1.1.11
10.1.1.13 10.1.1.13 10.1.1.13 10.1.1.13
10.1.1.255.1 10.1.1.255.255 10.1.1.255.1 10.1.1.255.255
10.1.1.17 10.1.1.17 10.1.1.17 10.1.1.17
sh-4.4#
```

Служебные порты

- UDP/2046,2048,2050
- TCP/2047,5100,10092
- TCP/5000-5003
- TCP/80*



Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **corpportal.local**

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Перезагрузить

Сведения

Замена координатора



Перепрошивка

- Неподдерживаемая платформа
- Неверно настроенный BIOS
- Аппаратные неисправности
- Некорректный DMI

```
>> success.
>> Mounting /run...
>> success.
>> Mounting /tmp...
>> success.
>> Creating devices...
>> Loading modules...
>> Waiting 3 seconds...
>> Init runs at console '/dev/console'
>> This is hw1000 platform (x86_64)
>> Keyboard lock patch is present
>> Waiting for disk devices to settle...
Automatic installation is disabled
tmpfs on / type tmpfs (rw,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /tmp type tmpfs (rw,relatime)
udev on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=10240k,nr_inodes=1001659,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
Installation device: /dev/sdb1
tmpfs on / type tmpfs (rw,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /tmp type tmpfs (rw,relatime)
udev on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=10240k,nr_inodes=1001659,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
Installation device: /dev/sdb1
>> Mounting device /dev/sdb1 with installation files...
>> success.
>> Mounting MAIN filesystem (/dev/sdb1)...
>> success.
>> Creating tmpfs for caching in /cache (size: 140 MB)
>> Copying sysimg.dat file for caching (size: 75716 KB)...
>> File sysimg.dat successfully cached
>> Copying upning.dat file for caching (size: 66208 KB)...
>> File upning.dat successfully cached
>> Mounting system software image:
>> Mounting the squashfs system /cache/sysimg.dat on /mnt/sysfs
>> success.
Verified OK
Copy probed hardware profile to /usb/1
See verbose hardware detection report in /tmp/verbose.txt
Copy verbose hardware detection report to /usb/1
Installation on not supported platform ABORTED. Press ENTER to reboot.
```



To Be Continued...

Игорь Виноходов
tg: @Igor_CSE

Бонус!

Защищенный Интернет-шлюз

