Содержание

2 Stingray Service Gateway implementation

Migrating from CentOS 8.x to VEOS 8.x

Due to the fact that Red Hat will early end support for CentOS 8 at the end of 2021, VAS Experts offers a strategy to continue using Red Hat as a Control Plane.
The transition to the new version of the OS is planned as a regular update (without reinstallation), within the framework of active technical support.

The transition to VEOS 8.6 (VAS Experts OS) will be phased in:

1. **January 2021** - Switching to the VAS Experts repository at the end of the release of patches for CentOS 8.5, does not require reinstalling the current CentOS packages
2. **February 2021 - May 2029** - Get kernel and OS component updates based on original RedHat 8.6, 8.7 and etc. from the new VEOS repository before the end of support for RedHat8. Version numbering will be identical to RedHat8.x packages
3. Creating a distribution kit for the initial installation of the OS - **the deadline will be determined in 2022** , but for now the initial installation is performed from the CentOS 8.5 installation disk and the subsequent switching of the repository

If you received a ready-made system from us, then immediately refer to the connection schemes. Otherwise, you need to independently install the VEOS 8 operating system on your server and provide us with remote SSH access and root rights to install and initially configure the platform. After completing the work, remote access can be closed.

2.1 Preparing the server and installing CentOS 8.x

1. Before rack-mounting the server, make sure it meets necessary requirements. If any discrepancies are found at this stage, contact VAS Experts technical support to promptly resolve the issue.
2. Install the latest version of CentOS 8.x using the link: **ISO CentOS 8.x minimal**

- When partitioning a disk:

```
 ~ 20 GB for root partition
the rest of the space can be allocated for the /var directory
The Stingray SG partition does not use swap, but it may be required for
system tasks, so 4GB can be allocated
```

- Disable Hyper-threading in BIOS

2.2 Pre-configuring CentOS 8.x

1. Create a **vasexpertsmnt** user:

```
adduser -m -G wheel -u 3333 vasexpertsmnt
```

2. Set a **complex** password for the user **vasexpertsmnt**:

```
passwd vasexpertsmnt
```

For convenience, you can generate a password using openssl:

```
openssl rand -base64 15
```

3. Save the password for **vasexpertsmnt**.
4. Set permission for users of the wheel group to use all commands on behalf of all users, for this you need to add to */etc/sudoers* the line:

```
% wheel ALL=(ALL) NOPASSWD: ALL
```

5. To provide remote access via SSH and set restrictions on valid IP addresses from the list:

```
 45.151.108.0/22, 94.140.198.64/27, 78.140.234.98, 193.218.143.187,
93.100.47.212, 93.100.73.160, 77.247. 170.134, 91.197.172.2,
46.243.181.242, 93.159.236.11
```

```
iptables -A INPUT -m conntrack --ctstate RELATED, ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -s 45.151.108.0/22 □□-m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 94.140.198.64/27 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 78.140.234.98 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 193.218.143.187 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 93.100.47.212 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 93.100.73.160 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 77.247.170.134 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 91.197.172.2 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 46.243.181.242 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 93.159.236.11 -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j DROP
service iptables save
```

If you are using firewalld:

```
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "45.151.108.0/22" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "94.140.198.64/27" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "78.140.234.98" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "193.218.143.187" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "93.100.47.212" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "93.100.73.160" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
```

```
"ipv4" source address = "77.247.170.134" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "91.197.172.2" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "46.243.181.242" service name = "ssh" accept'
firewall-cmd --permanent --zone = public --add-rich-rule = 'rule family =
"ipv4" source address = "93.159.236.11" service name = "ssh" accept'
firewall-cmd --reload
firewall-cmd --zone = public --remove-service = ssh --permanent
```

!Save your settings as the server will be rebooted during installation!

After making sure that remote access via SSH is provided, send to technical support of VAS Experts (Service Desk) file an application for installation of the Stingray SG DPI license with the password and username for SSH access.

The initial setup of the DPI platform is carried out by engineers VAS Experts technical support or her partners.

Do not update the operating system kernel until the system is activated updates, this may cause the network card driver to fail [1)]

Further settings are made depending on which components you plan to use, their descriptions are presented in Section 3 in the respective components.

1)

Troubleshoot