Содержание

2 Stingray Service Gateway implementation

If you received a preinstalled system from us, please immediately refer to the Appliance installation instructionsection.
Otherwise, you need to install the VEOS operating system on your server yourself and give us remote SSH access and root rights to perform the installation and initial configuration of the platform. After the work is completed, the remote access can be closed.

2.1 Preparing the server and installing VEOS

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 VEOS using the link.

- 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 VEOS

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.

Installation of the Stingray software is carried out by engineers or by yourself

according to the instruction: Instructions for installing the Stingray software using the script.

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 use cases you plan to use.

2.3 Migrating from CentOS to VEOS

Due to the fact that Red Hat discontinued support for CentOS 8 at the end of 2021, VAS Experts offers a strategy for the continued use of Red Hat as Control Plane.
The transition to the new OS edition is planned in the form of an in-house upgrade (without reinstallation), within the framework of active technical support.

1)
Troubleshoot